NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PERFORMANCE AND USAGE OF BIOMETRICS IN A TESTBED ENVIRONMENT FOR TACTICAL PURPOSES

by

Marianna J. Verett

December 2006

Thesis Advisor:	Alex Bordetsky
Second Reader:	David W. Netzer

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Performance and Usage of Biometrics in a Testbed Environment for Tactical Purposes			**5. FUNDING NUMBERS**
6. AUTHOR(S) Ms. Marianna Jane Verett			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Naval Postgraduate School's (NPS) Tactical Network Topology (TNT) experiments seek to develop, implement and identify sensor-unmanned vehicle network, and network centric operations to assist DoD warfighters in the Global War on Terrorism (GWOT). Using biometric data for rapid identification of High Value Targets (HVT) in ground and Maritime Interdiction Operations (MIO) is critical to the emerging special operation concept. The goal is to explore solutions and operational constraints associated with biometrics data analysis and rapid identification by means of adhoc self forming sensor unmanned vehicle (UV) wireless networks.

The objectives of this thesis are to look at how biometrics has performed in a testbed environment that is simulating a real special operations environment in theatre. This thesis is meant to explore and explain the biometrics process that was conducted on top of the tactical network and evaluate its performance.

This thesis provided the process model for biometrics identification in the tactical networks environment. This thesis also evaluated the length of time that it took to transmit the fingerprint data from the field to the ABIS database, with an identification result then sent back to the field. The longest time that was observed was 70 minutes (using low bandwidth Satellite communications), while the shortest time was 4 minutes for reachback to ABIS and 2 minutes for a local database.

14. SUBJECT TERMS Biometrics, Automated Biometric Identification System, American National Standards Institute, National Institute of Standards and Technology, Electronic Biometric Transmission Specification, Electronic Fingerprint Transmission Specification, Cross Match, Tactical Network Topology, 802.16, Mesh, Iridium Satellite, Unites States Special Operations Command, Maritime Interdiction Operations	**15. NUMBER OF PAGES** 91
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

PERFORMANCE AND USAGE OF BIOMETRICS IN A TESTBED ENVIRONMENT FOR TACTICAL PURPOSES

Marianna J. Verett
Civilian, Naval Postgraduate School
B.S., California State University, Long Beach, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 2006

Author: Marianna Verett

Approved by: Dr. Alex Bordetsky
Thesis Advisor

Dr. David W. Netzer
Second Reader

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Naval Postgraduate School's (NPS) Tactical Network Topology (TNT) experiments seek to develop, implement and identify sensor-unmanned vehicle network, and network centric operations to assist DoD warfighters in the Global War on Terrorism (GWOT). Using biometric data for rapid identification of High Value Targets (HVT) in ground and Maritime Interdiction Operations (MIO) is critical to the emerging special operation concept. The goal is to explore solutions and operational constraints associated with biometrics data analysis and rapid identification by means of adhoc self forming sensor unmanned vehicle (UV) wireless networks.

The objectives of this thesis are to look at how biometrics has performed in a testbed environment that is simulating a real special operations environment in theatre. This thesis is meant to explore and explain the biometrics process that was conducted on top of the tactical network and evaluate its performance.

This thesis provided the process model for biometrics identification in the tactical networks environment. This thesis also evaluated the length of time that it took to transmit the fingerprint data from the field to the ABIS database, with an identification result then sent back to the field. The longest time that was observed was 70 minutes (using low bandwidth Satellite communications), while the shortest time was 4 minutes for reachback to ABIS and 2 minutes for a local database.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like thank the Lord, who has blessed me and has makes all things possible. I would like to thank my family, especially my parents, who have constantly encouraged me during my master's journey. My close friends, Sarah, Ryan, Joanne, Amy, Briana, and Sommer thanks for putting up with me these past few years. There is absolutely no way I could have finished without my family and friends love and support.

I would like to mention those who work at the Biometrics Fusion Center. Kim Woods, Alan Viars, and Al Hernandez have helped and directed me in the right direction during this process.

Dr. Alex Bordetsky, thank you for seeing me through my endeavor of biometrics to the finish. I could not have done it with out your involvement and guidance.

Last, but definitely not least is Dr. Dave Netzer. I would like to express my appreciation for your patience, kindness, respectfulness, flexibility, and overall support of myself, my class work, and my thesis work. You made this possible for me. It has been an absolute pleasure to work with you and to be involved in this program you created. Your leadership and dedication in the USSOCOM-NPS Field Experimentation Program is why it is so successful.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Unites States Special Operations Command (USSOCOM) - Naval Postgraduate School (NPS) Cooperative Field Experimentation Program called, Tactical Network Topology (TNT) seeks in part to develop, implement, and identify sensor-unmanned vehicle network, and network centric operations to assist DoD warfighters in the Global War on Terrorism (GWOT). Using biometric data for rapid identification of High Value Targets (HVT) in ground operations and Maritime Interdiction Operations (MIO) is critical to the emerging special operations concept. The goal is to explore solutions and operational constraints associated with biometrics data analysis and rapid identification by means of adhoc self-forming sensor, unmanned vehicle (UV) wireless networks.

A. PURPOSE

Security is of the utmost importance and the means for obtaining it is in constant research. The use of biometrics can help with security for both the private and military sectors. Being certain of a person's true identity is the key. This is not as easy as it may seem. Even if perfect computers and applications were created that never made mistakes and would allow you to positively identify someone, there still is the issue of a "link" back to the huge database that stores identities. Unless you have a portable local database that allows you to identify a person on the spot, there is an unprecedented need for reachback to the main database. Only limited situations will allow for one to know which individuals need to be readily available in a portable database. A more common situation will call for collection of biometrics and then to send the file containing the unique character information back to the national or international central database. The value of communications and networks cannot be under estimated in this biometric equation.

B. OBJECTIVES

The objectives of this thesis are to look at how biometrics has performed in a testbed environment that is simulating a real special operations environment in theatre. This is necessary because the quicker a warfighter is in identifying an HVT and determining that the person needs to be detained or not, the quicker the warfighter can get

out of harms way. This thesis is meant to explore and explain the biometrics process that was conducted on top of the tactical network and evaluate its performance.

C. RESEARCH QUESTIONS

The primary research question is: When biometrics are implemented into a concept of operations (CONOPS), how beneficial is it to the warfighter? To answer this question, we will need to:

- Analyze areas of information and communication technology relevant to the (CONOPS) within the TNT testbed.
- Describe operational solutions for using and sharing biometric data in Intelligence, Surveillance and Reconnaissance (ISR) and MIO missions.
- Identify biometric technologies to meet the user needs.
- Identify and recommend DoD strategic technology initiatives that could effect the types of biometrics used.
- Identify measures of performance (MOP) for biometrics networking

D. SCOPE

This thesis will provide a broad overview of the TNT testbed with a focus on different realms of biometrics and then explain why the specific biometric application of fingerprinting was chosen and in what environment it was utilized.

E. METHODOLOGY

This thesis will use research from past biometrics testing in TNT experiments. It will also include data from actual executed CONOPS and from interviewing professors, students, Special Operations Forces, and employees of the DoD Biometrics Fusion Center.

F. THESIS ORGANIZATION

Chapter I describes the purpose, objectives, research questions, scope, methodology and organization of thesis.

Chapter II explains the history of the field experimentation program at the Naval Postgraduate School. It describes in detail the goals of each type of experiment and accomplishments that have come from the program, especially those that led to Biometric Identification integration.

Chapter III defines biometrics into two categories, physiological and behavioral, and gives examples of both. It specifies that biometrics are used for identifying and authenticating and why this is important in the GWOT.

Chapter IV discusses the ANSI and NIST standards and methodologies. This chapter spells out the difference between the CJIS/FBI – IAFIS and the DoD BFC – ABIS. It compares EBTS/ EFTS and gives examples of both. It will also clarify the different categories of fingerprints and different categories of submissions.

Chapter V gives the results from using the BFC ten-print device in a field environment. It explains how this could improve or degrade the effectiveness for the warfighter. It also summarizes the conclusions of this thesis and offers recommendations for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND OF THE NAVAL POSTGRADUATE SCHOOL FIELD EXPERIMENT PROGRAM

The Naval Postgraduate School faculty and students initiated a program of field experimentation in fiscal year (FY) 2002. In FY 2003 the experimentation transitioned into the Surveillance and Target Acquisition Network (STAN), with a primary focus on USSOCOM requirements. It was then that it took shape and started to form into a program that gained involvement from multiple departments within the school. To date the experimentation program has had over 30 faculty involved and has over 60 students who have graduated with STAN/TNT theses. Because NPS has a Joint focus, students from all services (Navy, Army, Air Force, Marine Corp.) and many foreign officers are involved. A unique benefit is that most of those students have valuable operational experience that they bring to the table. Through the years USSOCOM and the different Component Commands (USASOC, AFSOC, NAVSOC, and JSOC) have come to participate in and support the field experiments. There are many other government agencies, contractors, and private companies that also support this program.

A. STAN

Surveillance and Target Acquisition Network (STAN) was formed by the Dean of Research, Dr. David W. Netzer and a student, Christopher Manuel, who was the first Chief Warrant Officer to attend NPS. CW2 Manuel, helped to create the first prototype called Remote Observation Video Encoded Receiver (ROVER). This device's purpose was to provide Special Forces soldiers the means to receive Predator video on the tactical battlefield. This had the potential for providing the solider not only red force tracking, but blue force tracking also. "The motivation for providing friendly force positions to attack aircraft comes from the untimely death of CW2 Stan Harriman (after whom the network was named), killed by an AC-130 H in Afghanistan on 2 March 2002." (Manuel, 2004) "Soldiers, commanders, and members of Other Government Agencies (OGAs) considered Predator video delivered at the tactical level as "leap ahead" technology" (Manuel, 2004). (ROVER is now in its third iteration and has high level support.) CW2 Manuel felt strongly that there was a need for better situational awareness (SA) via commercial off the shelf (COTS) products to prevent fratricide. The main objective for STAN was "meant to reduce soldiers load, increase combat effectiveness, provide

situational awareness, increase standoff, reduce reliance on satellites, increase survivability, reduce fratricide find and fix enemy personnel and equipment." (STAN 6 Brief)

Figure 1. Example of what current SOF warfighters have to carry into battle

One of the main accomplishments of STAN was the creation of Inter-4's lightweight handheld PDA device, called the Tacticomp (see Figure 2). The Tacticomp allows a solider to send or receive video, data, and voice with or without infrastructure (Manuel). It is combat ready, in that it has been demonstrated to be ruggedized to the point of withstanding a 22-caliber gunshot. The Tacticomp graphically displays its location and the location of other devices that are a part of that network in its SA screen. When using a MESH (non-infrastructure) wireless card it has the ability to join a network ad hoc by self-forming and self-healing. The range of this device varies depending on which type of wireless card is used and if there is amplification.

Figure 2. Inter-4's Tacticomp

Many other notable accomplishments took place during the STAN experiments. One notable one is the installation of the long-haul, high bandwidth wireless backbone between NPS in Monterey and Camp Roberts. It's a 100 mile distance using OFDM/802.16 technology. This allowed the network operation center (NOC) in Monterey to see exactly what was going on at the tactical operation center (TOC) in Camp Roberts, and to participate interactively.

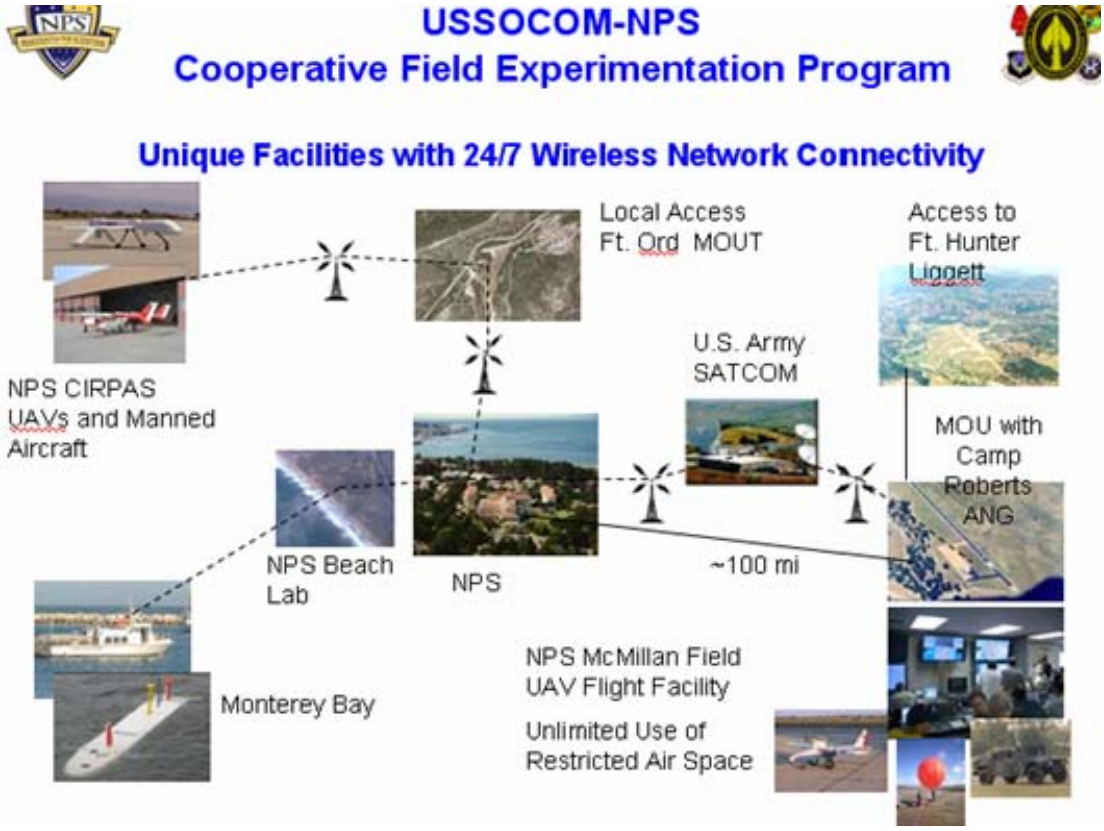

Figure 3. 100 mile backbone from Monterey to Camp Roberts and various sites

Another was the successful use of Red Team Intent (RTI), which is a program that NPS Professor John Hiles created in conjunction with a Lawrence Livermore National Laboratory (LLNL) program called SONOMA. It takes a video that is surveying a city and allows the operator to input a particular pattern to look for. For example if it is known that a driver of a car which slows down to five miles per hour for more than 100 feet is suspicious activity, then the program will highlight the paths of all vehicles that have this exact activity. The clever part about this program is once the pattern has been triggered, one can rewind the video and see where the suspicious vehicle came from.

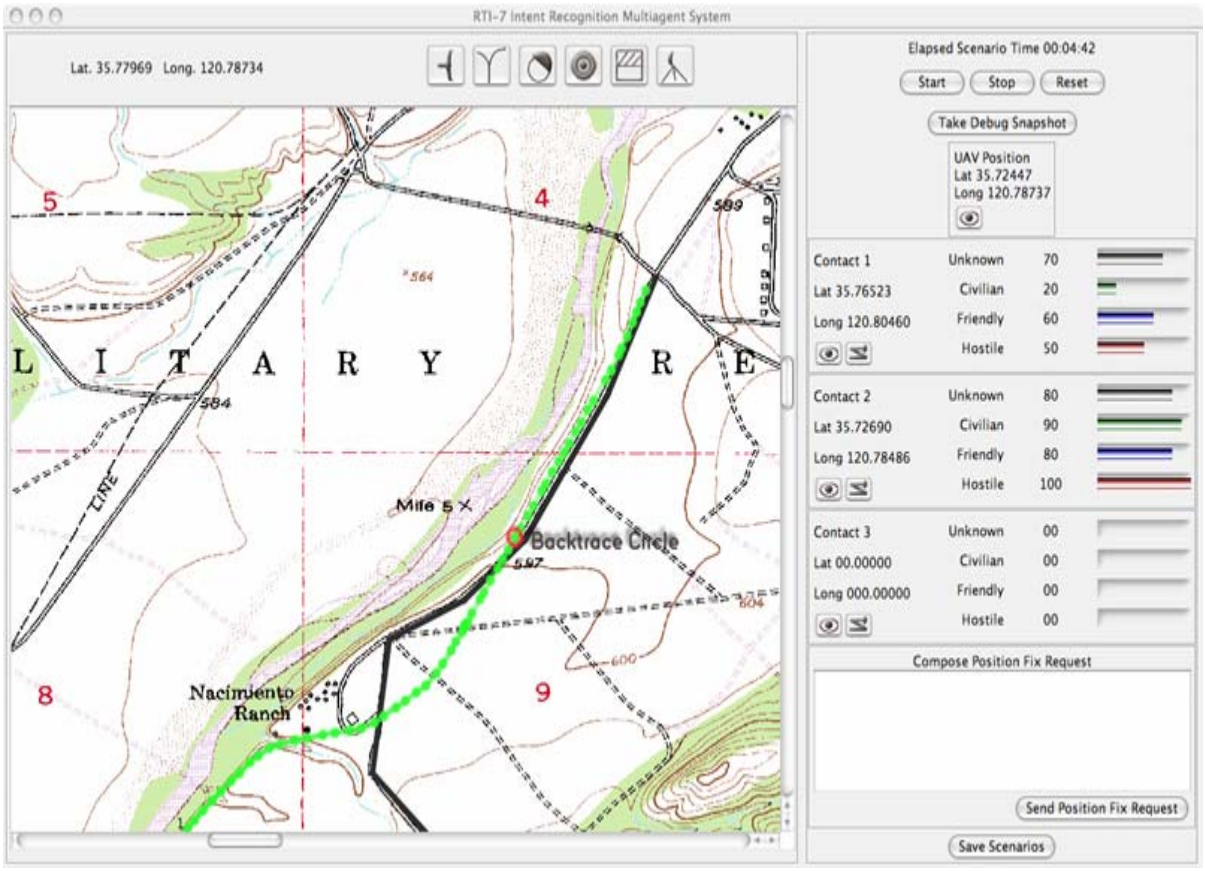

Figure 4. RTI screen shot

Additionally, there were ship-to-shore experiments conducted using the 802.16/OFDM technology. The results were good considering that 802.16 was not designed to operate near the water surface, which adds unfavorable atmospheric and surface conditions. The boat was able to go 13 km out to sea and still get connectivity with the NOC. Video and VoIP were passed at 12Mbs. These are just a few of the many and varied accomplishments that came to fruition from the STAN experiments.

B. TNT

Starting in FY05 STAN transitioned again and became the Tactical Network Topology (TNT) program. The name change was made primarily because USSOCOM developed programs of record from STAN efforts and a wider range of technologies were being explored. With the transition of STAN to TNT came more involvement from the Component Commands. Now the scenarios and experiments that are utilized are developed from this working group of NPS, USSOCOM J9, and all USSOCOM Component Commands. The more mature technologies are usually carried from one set

of experiments to the next. The goal of having a Cooperative Field Experimentation Program is to "focus on identifying key gaps and deficiencies resulting from applications of advanced technology, particularly network communications, unmanned systems and net-centric applications". (TNT 05-4 AAR) The quarterly field experiments have the following structure:

- One week in Camp Roberts:
  - 1-2 days: setting up Ground Control Stations (GCS's), networks, etc.
  - 1-2 days: conducting individual experiments which evaluate new and emerging technologies.
  - 2 days: running scripted scenarios to evaluate integrated technologies in a tactical environment.
  - 1 day: engineering day – evaluating and deciding upon which technologies will be used in following experiments.
- 3 days of Autonomous Underwater Vehicle (AUV) and Maritime Interdiction Operations (MIO) in Monterey Bay or off of San Francisco Bay:
  - 1 day: set up
  - 1-2 days: running MIO experiment and testing underwater technologies

An example of a scenario that occurs in Camp Roberts for TNT could involve a convoy of hummers consisting of an ODA (Operation Detachment Alpha) team that has biometrics equipment. The ODA stops at a set of buildings and secures one, finds potential WMD (weapons of mass destruction) material in another building and leaves a surveillance camera that detects motion. In the third building the ODA team finds an HVT (high value target) and brings the suspect out to the LRV (Light Reconnaissance Vehicle) where the biometric equipment is located and takes the HVT's rolled finger prints or ten-print. LRV personnel send the ten-print, one MB file to the TOC and from the TOC, it is sent up the 100 mile 802.16 backbone to the NPS NOC. Once at the NOC the ten-print is sent via hardware VPN (virtual private network) to the Biometrics Fusion Center (BFC). BFC then provides the positive identification of the HVT. The HVT is detained. An RFID (radio frequency identification) sensor detects a threat vehicle, which shows up in the SA in the TOC. The TOC provides the location to an unmanned aerial system (UAS) that will find and track the threat vehicle, providing surveillance video to

the TOC. The video shows that the threat vehicle has come to a stop and the driver has exited. TOC directs the UAS to fly high and continue surveillance, while the NPS SUAV (small unmanned aerial vehicle) is directed to fly to the threat vehicle and lock video on target. Then the video is fed into software which will determine the coordinates of the target within a one to two meter accuracy. Once the GPS coordinates are determined the SUAV lands and the MMALV (micro morphing air-land vehicle) flies out to the vehicle, lands, and crawls under the vehicle. The camera, which normally faces forward during flight, flips up and gathers images of the IED that has been placed in the underbelly of the threat vehicle. TOC commander confirms this IED material and sends directions to the ODA to return to the TOC on an alternate route, so not to pass by the IED vehicle. Some high level objectives for a scenario of this type would be:

1. Determine the effect of different wireless communication methods (SOF-TOC and TOC - remote sites) on mission effectiveness and duration during a HVT search mission.

2. Determine utility of multiple UASs, ground sensors, precision jammers, and SIGINT target locaters integrated in the Tactical Network for preventing IED attack. (TNT 05-4 Scenario).

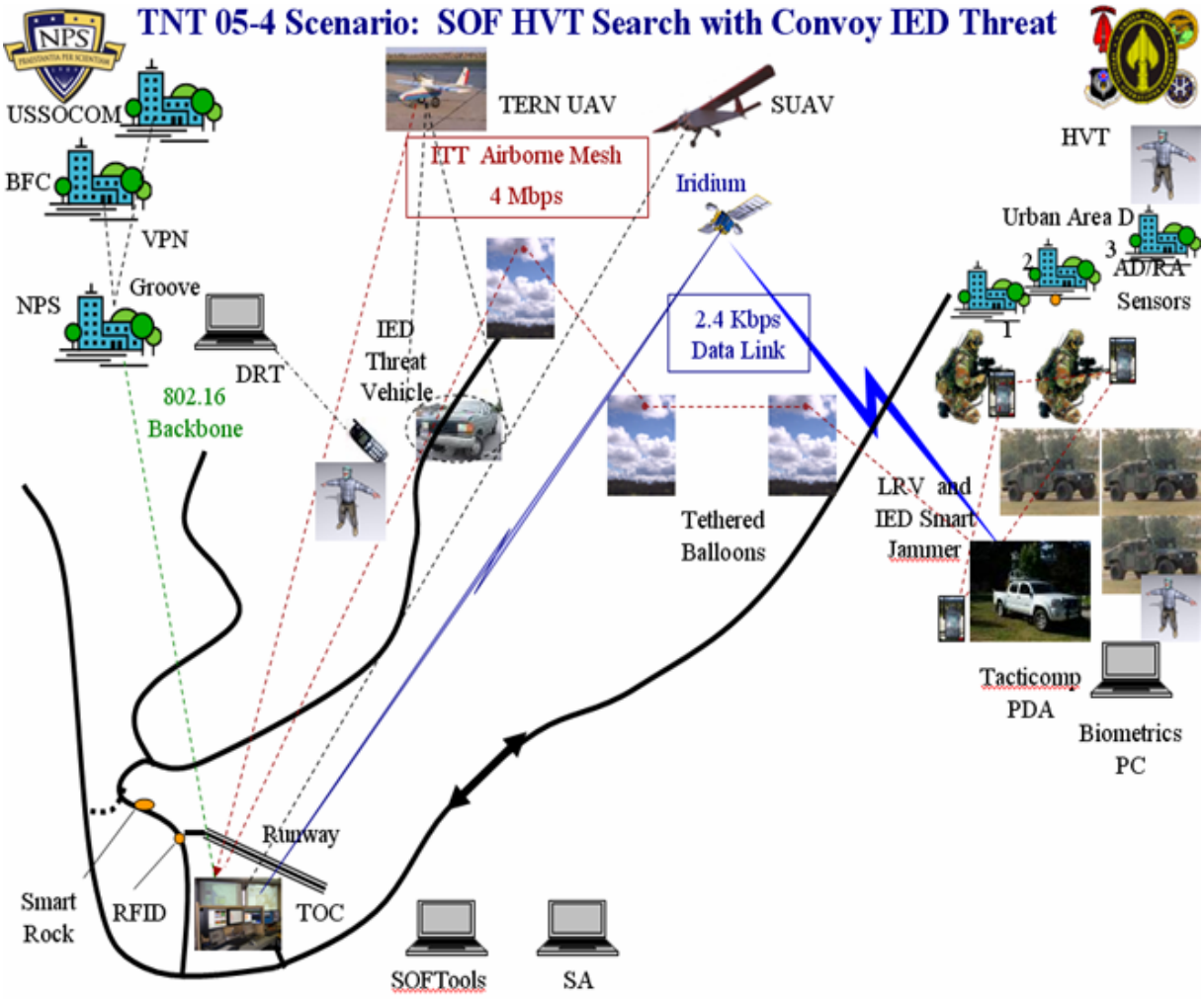

Figure 5. Pictorial description of a possible TNT scenario

The experiments that have been conducted during the 3 day maritime section of the TNT have been varied. The AUV portion has included experiments that examined:

- Navigation, communication and control of multiple vehicles (via acoustic modems)
- Obstacle avoidance (via forward looking sonar)
- Mine locating in littoral (TNT05-1 Brief, slide 7)

Figure 6. NPS AUV Aeries

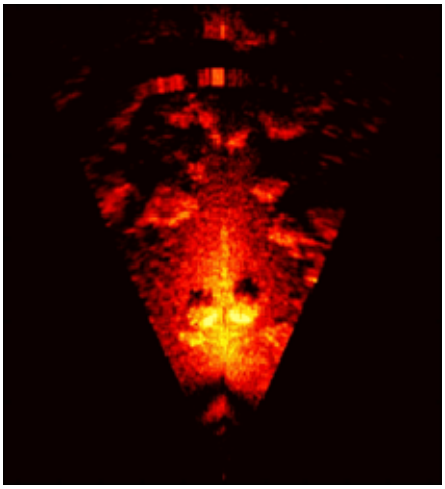

Figure 7. Aries forward looking sonar image

Most of these tests have been done with naval special operations missions in mind. During combat swimming situational awareness is greatly desired. Inter-4 made an underwater PDA, called the NAVBOARD to give the swimmer way points to follow while underwater. NPS modified the NAVBOARD to permit situational awareness (SA) to be sent to the submerged swimmer via a wireless network. Images from aerial surveillance of the beach and /or sonar images of mines and their location in the littoral could be sent to the swimmer with only a small antenna on the surface.

This device had varying degrees of success, while the network performed reasonably well, the device could not made water tight.

The other facet of the maritime operations is evaluating technologies that can be used in maritime interdiction of a suspect vessel. In these types of operations

communications between the originating ship and the boarded ship is imperative. This has been one of main focuses of the experiments, and we have used a man-packable form of 802.16. It is a portable version of the OFDM technology that can be stored in a backpack and carried on board the target ship where it is setup to link back to the originating ship.

Once reliable ship-to-ship and/or ship-to-shore comm's has been setup, then a MESH network is set up on the boarded ship to connect all personnel and equipment on the deck. With MESH networking up and running the BFC connects their equipment through it and takes fingerprints of all personnel on the boarded ship. Now that the deck communications has been setup then Lawrence Livermore National Laboratory (LLNL) goes below deck and sets up their Ultra Wide Band (UWB) network. The main advantage of UWB is that it has LPI/LPD (low probability interception/low probability of detection) covertness. Evaluated in the experiments was the through-wall performance of the UWB (low frequency) for below deck communications. Also evaluated were the LLNL technologies for the detection and identification of sources of radiation and their Easy Livermore Inspection Test for Explosives (ELITE) shown in Figure 8; a colorimetric explosives detection system that detects over 25 explosives and their radiating precursors.

Figure 8. Example of Elite Detection

The high level objective of the MIO experiment conducted in TNT 05-4 was to demonstrate capability of network integration and distributed sharing for (utilizing) new radiation detection technology and remote instrument expertise and biometrics databases which are geographically distributed. Explore integration of self-forming wireless networks, including the ultra-wideband links for ship metal structures penetration, (together) with advanced collaborative technology tools, shared situational awareness display, and GIG/DREN wide area connections for bringing the radiation source analysis and biometrics identification remote experts to the support of the boarding party within the real-time constraints critical to the boarding party success.

Figure 9. Overview of MIO exercise

C. ROLE OF BIOMETRICS

The future of the field experimentation program is good. Continued funding from USSOCOM and other sources appears to be in place. Structurally, the program will probably follow a format similar to TNT 06-2 :

- 22-24 Feb.: RHIB or equivalent out to sea with airborne relay for reachback or AUV work in Monterey Bay
- 25 Feb – 3 Mar: Multiple coordinated SOF operations: Camp Roberts, Avon Park, San Diego, and Missoula
- 5-7 Mar: MIO exercise in Alameda Island and Suisun Bay.

New elements have been added to TNT 06 experiments. Doing two separate maritime experiments in one quarter has yet to be done, but if one considers everything that needs to be evaluated it may occur. Running multiple missions in multiple locations (i.e. Camp Robert and Avon Park) simultaneously is a new element, but desired by USSOCOM.

One needs to investigate how biometrics works on top of an evolving network infrastructure. The variables can include user and network performance, plus operational procedures.

III. BIOMETRICS FOR TACTICAL NETWORKS

A. DESCRIPTION

A descriptive definition of Biometrics can be found in the Department of Defense Biometric Management Office, Biometrics Fusion Center (DoD BMO, BFC) website www.biometrics.dod.mil. It says that biometrics should be measurable, physiological and/or behavioral characteristics that can be used to verify the identity of a person. This chapter will explain the two different type of biometrics and then give examples of each.

B. DIFFERENT TYPES OF BIOMETRICS

As mentioned above, the different types of biometrics fall into two categories: Physiological and Behavioral. Physiological biometrics is based upon the recognition of physical characteristics, such as fingerprints, hand geometry, iris recognition, and facial recognition (Layman's, 2005). Behavioral biometrics can be described not as a physical characteristic, but are traits that are learned or acquired over time as differentiated from physical characteristics. Some examples are: voice, signature or keystroke recognition (Layman's, 2005).

1. Physiological Biometrics

Physiological biometrics are physical traits or attributes that everyone has. Fingerprints, irises, and faces are not easily altered. This is why these are viable options for identification and merit further research.

a. Fingerprinting

Fingerprinting is the most common form of biometric used to date. It has been in forensic use for over a hundred years. The reason being is that fingerprints are unique to each individual and for the most part do not change over one's lifetime (Polemi, 1997). Fingerprints patterns are classified by three categories (shown in Figure 10): arch, loop, and whorl.

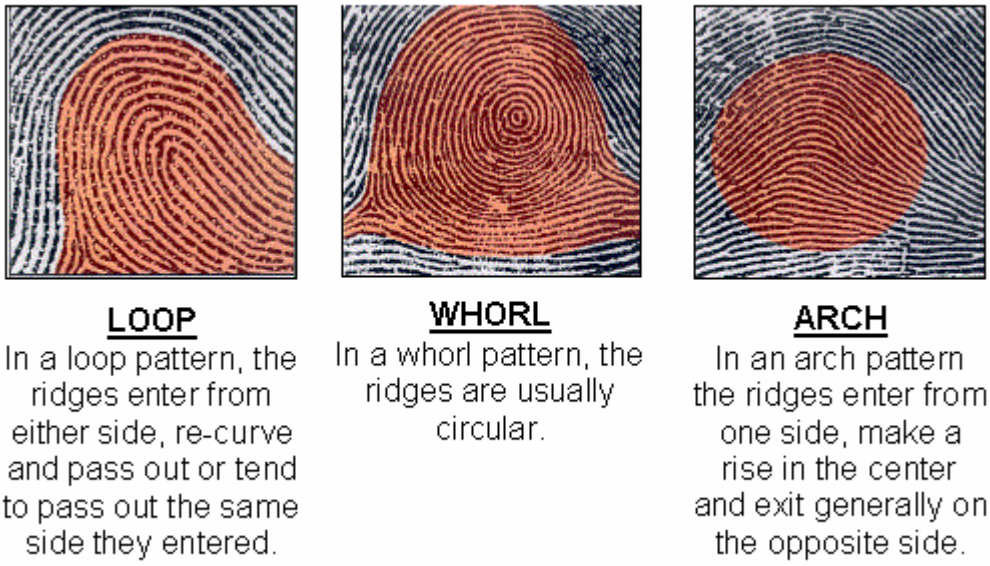

Figure 10. Example of the three different fingerprint patterns (Patterns, 2006)

Characteristics of fingerprints that make them discrete are called minutiae, forks, or endings found in the ridges and the overall shape of the ridge flow. (Polemi, 1997) These distinctive qualities are captured either by one placing their fingers on a specialized high resolution scanner or the old fashion way (i.e. paper and ink). Once the digits are digitally captured they are entered into a database. Standardization of capturing methods and information deposits into databases are necessary requirements in order to match quickly and correctly.

The advantages of using fingerprinting is that it a proven biometric (for multiple prints) and it is usually accepted in our culture. The disadvantage is that unless it is a latent print being lifted of an item, the finger-printed person physically knows that there is an attempt to identify him.

There are many areas of application for fingerprinting. The following are industries that use fingerprinting:

- Government Agencies
- Banking
- Medical & Insurance Industry

- Information Security
- Identity Authentication
- Police Department
- High Power Reactor Stations
- Immigration and Naturalization Services
- Airport Traffic Security
- Welfare & Unemployment Benefit Recipients
- Identification of Missing Children
- Database management systems
- Computer access or transaction control
- Computer Database Security Control
- Physical Access Control (Polemi, 1997)

With so many ways to apply fingerprinting, it will continue to grow as one of the leading forms of biometrics, especially ten-prints where misidentification is less likely.

b. Iris

Iris scanning is considered to be one of the most reliable methods for identifying someone. "The human iris is an annular region between the black pupil and the white sclera." (Wang, 2003) It is the texture of the iris that provides the unique quality. Other characteristics that make the iris inimitable are connective tissues, collageneous stromal fibres, ciliary processes, contraction furrows, rings and colorations. (Polemi, 1997) All together there are over 400 distinctive characteristics in the iris alone (Iris, 2006). "Due to these unique characteristics, the iris has six times more distinct identifiable features than a fingerprint" (Iris, 2006).

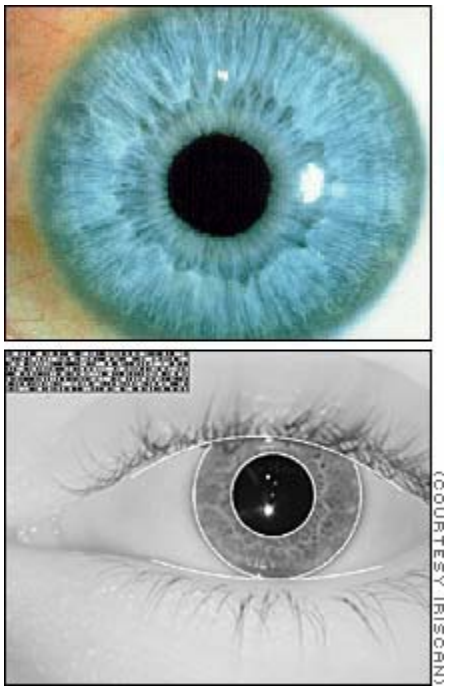

Figure 11. Iris scanners looking for unique identifiers (Iris Recognition, 2000)

An advantage of iris scanning is that it is protected from the external environment. It is impossible to modify surgically without risking vision, so ultimately there is a low risk of impersonation. One of the biggest benefits is that scanning and gathering iris data is done at a short distance without physically touching the subject (Polemi, 1997). Some disadvantages: susceptible to disease damage (i.e. cataracts), even though it can be done at a distance it is still considered to be intrusive and not very user friendly, high amount of both user and operator skill required, and inadequate funding from government and private sectors (Iris, 2006).

Possible places that iris scanning could be applied are at:

- Correction facilities
- Department of Motor Vehicle
- Military checkpoints
- POW facilities

c. Facial Recognition

Facial recognition is done everyday, by everyone. The Automated Identification and Data Capture Biometrics website states:

> Facial feature identification is inherent in all of us. Individuals can immediately distinguish among people just by looking at their face. As a result, facial feature identification is considered to be one of the most natural biometric technologies (Facial, 2006).

With the advent of cameras and other multimedia technology this form of biometric has become more popular. The procedure of conducting facial identification involves two processes: detection and recognition. In detection a camera needs to be able to identify within a frame of video or a photograph that there is a human face and then separate it from any other items that could be in that same image (Facial, 2006). At this point software is used to look at the face selected and pick out the identifying features, such as: size of nose, shape of eyes, chin, eyebrows, and mouth (Polemi, 1997). "After constructing an image of one's face, the software "cuts" away any background details leaving the image of one's face in a rectangle frame called a binary mask" (Facial, 2006). Using this binary mask enables the software to conduct the recognition portion of the process. Recognition is comparing the collected facial image against other faces that are held in a database. This is a simplified explanation of the process of facial recognition and it can be done in various ways.

Figure 12. Facial feature detection (Analyzing)

Advantages of facial recognition are: it is highly acceptable in this culture to be identified in this manner and it's noninvasive, it doesn't require any physical contact. A disadvantage of facial recognition is that some of the systems and software used can be ineffective if the angle, lighting, or facial expression that is captured is different than the coinciding image that is held in the database (Polemi, 1997). Another disadvantage is that the database needs constant updating because the aging human skeleton is constantly changing (Polemi, 1997).

This is a growing field, just a few areas of applications are:

- Banking
- Credit Card Companies
- Social Security Systems
- Airport Security
- Hospital / Health Care Institutions (Polemi, 1997).

2. Behavioral Biometrics

Behavioral characteristics are a reflection of an individual's psychological makeup, although physical traits, such as size and gender, have a major influence. These behavioral characteristics can be unique enough to measure and identify a person.

a. Signature

> The specific features of the signature and specific features of the process of signing one's signature are the two methods that signature identification analyzes. There are five main features that need to be measured, and they are speed, pen pressure, directions, stroke length, and the points in time when the pen is lifted from the paper (Signature , 2006).
>
> Signature identification devices also can analyze the "static" image of one's signature. In using the "static" image method, the signature identification device captures the image of one's signature and saves it for future comparisons to the stored template (Signature, 2006).

Advantages for signature identification is that signing is something that people have to do every day and is a part of our culture, therefore, this is an accepted biometric. A disadvantage is that this is not a suitable biometric to use in countries that have high illiteracy rate (Polemi, 1997).

b. Keystroke

Keystroke as a biometric is still underdevelopment. It measures typing characteristics of individuals. The following are examples of what is measured: keystroke duration, inter-keystroke times, typing error frequency, force strokes, etc (Polemi, 1997).

> Two kinds of systems are getting developed based upon static and dynamic verification techniques. The static verifier uses a neural network approach while the dynamic verifier is using statistics. The static approach is where the system analyzes the way a username or password was typed

using neural network for pattern recognition. Dynamic approach is where the system verifies the person continuously with any arbitrary text input. (Polemi, 1997).

This is an emerging technology and has much potential in any industry that utilizes computers/keyboards on a regular basis. Because it is not a mature biometric, at this point it would be very costly to invest in (Keystroke, 2006).

c. Voice

Voice or Speech identification analysis studies the sounds, phonetics, and vocals generated by a person. The individuality of these characteristics are produced by the mouth, nasal cavities, and vocal tract which is unique to everyone (Polemi, 1997).

A voice identification system requires that a "voice reference template" be created so that it can be evaluated against new voice entries. One must speak a set phrase several times so that the system can build the reference template. "Voice identification systems incorporate several variables or parameters in the recognition of one's voice/speech pattern including pitch, dynamics, and waveform" (Voice, 2006).

"There are five specific forms of voice identification technologies that are currently available or under development:

1. Speaker Dependent

This type of technology involves "training" the system to recognize your speech patterns. Systems employing this technique can hold a vocabulary of between 30,000 and 120,000 words. Best if used by a specific user.

2. Speaker Independent

This type of voice identification technology can be used by anyone without having to train the system. As a trade off, the vocabulary is smaller and error rates higher.

3. Discrete Speech Input

This environment involves the person speaking to make small pauses, as small as 1/10 of a second, between words. This allows the system to recognize where words begin and end.

4. Continuous Speech Input

Users can speak at a continuous rate but the voice identification software can only recognize a limited amount of words and phrases. This type of

technology is also referred to as "word-spotting" systems. They are called "word-spotting" because a user can be speaking in long sentences or phrases and the system will only recognize predetermined words.

5. Natural Speech Input

This is the most desired form of voice identification, but is still under development. Here the user is able to speak freely and the system is able to interpret and carry out commands on-the-fly." (Voice, 2006)

Advantages of using voice as a biometric is that it provides eyes and hands-free operation and is considered a "natural" biometric technology (Voice, 2006). Disadvantages are that it is not as accurate as other biometrics, if people are sick or unable to speak, that will affect the accuracy of identification. And verification of people who are under the influence, taking dental anesthesia, or have an oral obstruction, is extremely difficult (Polemi, 1997).

Some areas of application:

- Telephony (hands-free dialing)
- Used by disabled persons
- Used by physicians to record patient data and make records while conducting observations (Voice, 2006)

3. Other Biometric Areas

There are many other biometric areas not discussed in this thesis. There are so many, that the purpose of this chapter was to go into depth with just a few of them. Other biometric areas for research are:

- Hand Geometry – Vein Patters (Thermal)
- Retina
- DNA pattern
- Ear recognition
- Odor detection
- Sweat pores analysis
- Head analysis
- Gait

It is apparent that obtaining data for more than one type of biometric will significantly increase detection accuracy and speed.

C. IDENTIFICATION VERSUS VERIFICATION

Identification and verification produce two different results in the biometrics world. "During identification, the biometric system asks, "Who is this?" and establishes whether a biometric record exists, and, if so, the identity of the enrollee whose sample was matched. During verification, the biometric system asks, "Is this person who he/she claims to be?" and attempts to verify the identity of someone who is using, say, a password or smart card." (Identification, 2006)

Identification (1:N or one-to-many) in a biometrics system will search for a positive identification within a predefined group of individuals. The matching algorithm searches using a biometric sample given by the individual, through each record it has on file. This process is in general slower than verification. (Verification, 2006)

Verification (1:1 or one-to-one) in a biometrics system will search using a matching algorithm for positive identification using both a biometric sample and a unique user identifier (e.g. name). The matching algorithm searches all records on files and the result comes back as "Match" or "No-Match." This process is relatively simpler and faster compared to Identification. (Verification, 2006)

THIS PAGE INTENTIONALLY LEFT BLANK

IV. BIOMETRIC STANDARDS

Similar to what IEEE has done for networking and other applications, fingerprinting has also been standardized. This standardization includes metrics used to capture fingerprints and includes minimal requirements needed for the device used. This chapter is meant to briefly explain the standards and how they are meant to be used.

A. SUMMARY OF DOD ABIS

DoD ABIS stands for the Department of Defense Automated Biometric Identification System. This is used by the government entities. It is convenient because it is held within a centralized biometric database and can capture multiple types of biometric data (Overview, slide 3). It searches and matches biometric data automatically, and then it communicates with client applications (e.g., Biometrics Automated Toolset (BAT), Biometrics Identification System for Access (BISA)) (Overview, slide 3). A very important factor is that it easily exchanges data with other organizations (e.g., FBI and DHS) (Overview, slide 3). Implementation of DoD-specific data fields and transactions, support of existing transmission specifications, and the use a common data interchange format, are all within DoD ABIS to assure enterprise-wide interoperability (Overview, slide 3).

B. SUMMARY OF DOD EBTS

DoD EBTS also known as Electronic Biometric Transmission Specification, focuses on the transactions that are essential to interface with the DoD ABIS (Overview, slide 4). It actually enhances the FBI's EFTS (Electronic Fingerprint Transmission Specification). While still using many EFTS capabilities, it incorporates additional DoD-specific information (Overview, slide 4). It specifies more than just fingerprinting standards, but a variety of data types (e.g., iris and face) (Overview, slide 4). EBTS implemented ANSI/NIST ITL 1-2000 data formats, which will be explained later on in this chapter. Because future use will require programs or implementations that need additional functionality, EBTS has extensible domains. EBTS allows EFTS-complaint biometric submissions in order to remain compatible with the DoD ABIS. As stated in the DoD ABIS and EBTS Overview Version 1.0:

- "DoD EBTS transactions which are submitted to the FBI's Integrated Automated Fingerprint Identification System (IAFIS) will not be rejected
- IAFIS ignores additional DoD-specific information
- Equipment generating DoD EBTS transactions is EFTS-compliant" (Overview, slide 4).

To summarize this means that ABIS (via EBTS) is compatible with the FBI's IAFIS through EFTS. EFTS is expounded upon in section C.

C. SUMMARY OF FBI IAFIS / EFTS

FBI's EFTS (Electronic Fingerprint Transmission Specification) implements ANSI/NIST ITL 1-2000 data format, because compliance is required for information exchange with the Criminal Justice Information Services Division, which uses the Integrated Automated Fingerprint Identification System (IAFIS) (Overview, slide 5). EFTS accepts submission of fingerprints (10-prints, latent prints), mug shots, photos of scars, marks, and tattoos (Overview, slide 5). Submissions to FBI are called "transactions" and multiple Types of Transaction (TOT) are allowed (Overview, slide 5). EFTS transactions and data format elements are IAFIS-specific and therefore certain biometrics (e.g., iris) are not supported (Overview, slide 5). Below is a table that briefly compares and contrasts EBTS and EFTS.

	EFTS	*EBTS*
Name	Electronic Fingerprint Transmission Specification	Electronic Biometric Transmission Specification
Interfaces With	FBI IAFIS	DoD ABIS / FBI IAFIS
Use	Criminal Justice	Red Force Gray Force Blue Force
APPLICATION		
Submission	X	X
Storage	X	X
1:n Identification	X	X
1:1 Verification		X
BIOMETRIC MODALITY		
Fingerprint - 500 ppi	X	X
Fingerprint - 1000 ppi		X
Fingerprint - Latent	X	X
IMAGE		
Facial Image	X	X
Iris Image		X
Demographic data	some	more

Table 1. DoD EBTS/EFTS Comparison (From Overview, 2005)

The table above shows many differences between EFTS and EBTS. EBTS has military uses, where as EFTS is used in the Criminal Justice system. The significant difference between the two transmission specifications is that EBIS can be used for 1:1 Verification and has started use of Iris identification.

D. DOD ABIS/EBTS SPECIFICATIONS

ABIS is collocated with IAFIS, but is maintained by the BFC. It's important to note what the BFC's initiatives are:

- Test and Evaluation
- Policy Development
- Standards Development
- Education Program

- Knowledge Management
- Protection Profiles
- Product and Industry Research
- Implementation Support (BFC, 2006)

To visualize the flow of biometric initiatives, standards, and testing, please see Figure 13.

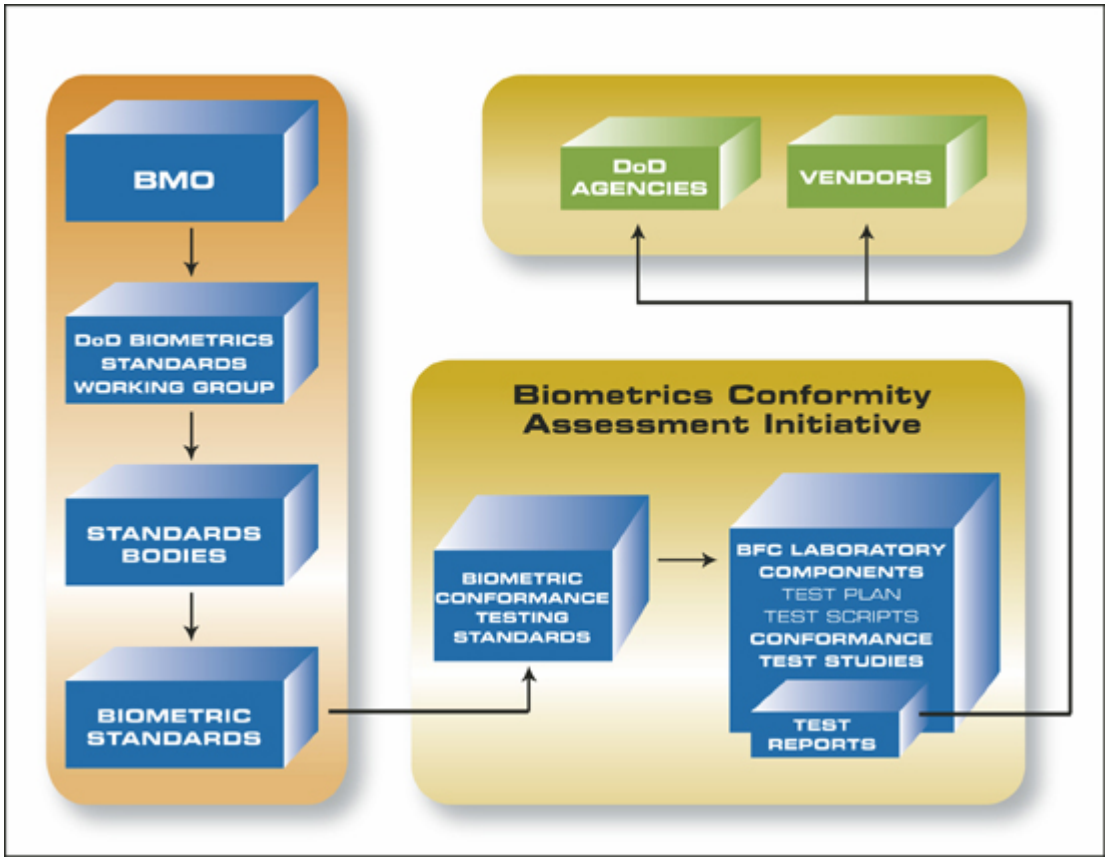

Figure 13. Flow of Biometric Conformity and assessment Initiatives (From BFC Standards, 2006).

The BFC, keeping with ANSI/NIST standards, has 3 different types of fingerprint storage within DoD ABIS. They are 10-print rolled fingerprint data, flat fingerprint data ranging between 1-10 flat prints, and latent fingerprints images (EBTS ver1.1, p3).

As shown in Table 2 there are several categories of use or submissions for EBTS. Below describes what each category means:

- Red Force, which searches for detainees, enemy combatants, enemy prisoners of war (EPWs), or persons of interest (known or suspected terrorists).
- Gray Force submission is used when military personnel are trying to identify someone at a check point type of situation or verifying third country nationals who are trying to work on a US military base.
- Blue Force is meant to identify and verify military and contractor personnel . It should be noted that ABIS does not contain the biometric files of US citizens.
- Latent submission is mainly used for forensic purposes. They are normally gathered after the fact, for example one could be lifted of an improvised explosive device (IED) (EBTS ver1.1, p3).

Each type has to be submitted to ABIS with an EFTS/EBTS, transaction of type. Table 2 specifies for each submission the corresponding transaction type. The type of submission is important because it qualifies the category in which the newly submitted fingerprints should be inputted. Tables 3 and 4 explain the submissions and responses/searches possible for each transaction type.

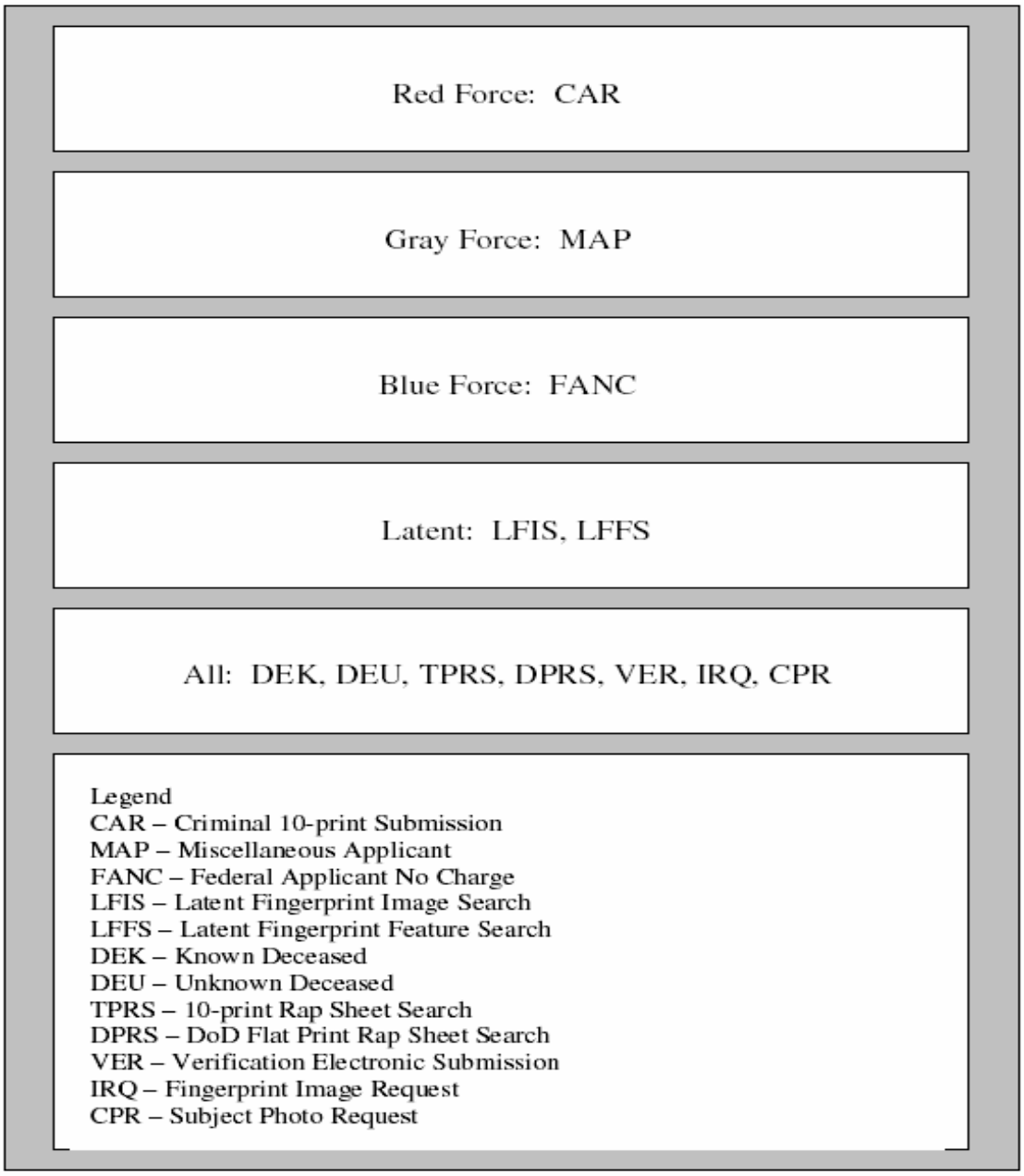

Table 2. Types of submission (From EBTS ver1.1, p5).

EBTS TOT	EBTS Transaction Name	DoD Implementation Notes
Electronic 10-print Submissions		
CAR	Criminal 10-print Submission (Answer Required)	Submission used for detainee or EPW.
FANC	Federal Applicant No Charge	Submission used as part of a background check for enlisting U.S. military, DoD civilians, and DoD contractors.
MAP	Miscellaneous Applicant	Submission used as part of a background check for local nationals and third country nationals who require access to U.S. military installations or other restricted areas.
DEK	Known Deceased	Submission used for deceased subject whose identity is known.
DEU	Unknown Deceased	Submission used for deceased subject whose identity is not known.
SRE	Submission Results - Electronic	Response containing an Ident/Non-Ident decision; will contain an electronic rap sheet if requested.
ERRT	10-print Transaction Error	Error response.
Remote 10-print Searches		
TPRS	10-print Rap Sheet Search	Performs a search only, non-retain, and can return an unconfirmed-identification ("yellow") identification.
DPRS	DoD Flat Print Rap Sheet Search	This is only used in special circumstances.
SRT	Search Result – 10-print	Response including a candidate list comprising names and DoD number of each candidate.
ERRT	10-print Transaction Error	Error response.
Remote Latent Print Searches		
LFIS	Latent Fingerprint Image Search	Used for latent image submission and searches.
LFFS	Latent Fingerprint Feature Search	Used for latent feature submission and searches.
LRE	Latent Result	Latent Response containing an Ident/Non-Ident decision.

Table 3. EBTS Types of Transactions (TOT) (Submissions and Responses) by Category (From EBTS ver1.1, p8).

EBTS TOT	EBTS Transaction Name	DoD Implementation Notes
ERRL	Latent Transaction Error	Error response.
Remote Requests for Fingerprint Images		
IRQ	Fingerprint Image Request	Request for identification information (flat prints, mug shots, demographic/biographic information).
IRR	Fingerprint Image Request Response	Response containing requested identification information (flat prints, mug shots, demographic/biographic information).
ISR	Image Response Summary	Response indicating that the prints were not on file with DoD ABIS.
ERRI	Image Transaction Error	Error response.
Electronic Criminal Subject Photo Searches		
CPR	Subject Photo Request	Request for mug shot photos on file with DoD ABIS.
PRR	Photo Response	Response containing requested identification mug shot photos.
Verification		
VER	Verification Electronic Submission	Used for 1:1 verification based on an identifier.
VRSP	Verification Response - Electronic	A verification response that contains Ident/Non-Ident information.
EVER	Verification Error Response	Error response.

Table 4. EBTS Types of Transactions (TOT) (Submissions and Responses) by Category Continued (From EBTS ver1.1, p9).

E. ANSI/NIST ITL 1-2000 DATA FORMAT

As explained at the beginning of this chapter there are standards that manufacturers have to follow if they are trying to build a biometric device. The Image Storage and Retrieval (ISR) devices need to be compliant with the ANSI/NIST (American National Standards Institute/National Institute of Standards and Technology) 1-2000 Data Format standards. This standard was approved in July 2000 and is currently undergoing revisions. ANSI/NIST formats were implemented in EBTS and EFTS. ANSI/NIST facilitates effective exchange of identification data between dissimilar systems, using the Common Biometric Exchange File Format (CBEFF). It also provides common format for data exchange (for example they do not have to use Cross Match equipment, as long as the equipment is ANSI/NIST compliant). This data format supports several modalities, such as fingerprint, palm, facial, and scar mark/tattoo images. In order to support all of this an extensible data encodings, or XML is used. Multiple modalities can be supported using standard biometric data formats

The following are some areas in which the ANSI/NIST goes into great detail:

- Transmitted Data Conventions
    - Byte and bit ordering
    - Grayscale data
    - Binary data
    - Color sequence
- Image Resolution Requirements
    - Both Scanner and transmitting resolution requirements
- File Description
    - File formats and contents
    - Implementation domains
    - Image designation character (IDC)

- Record Description
    - Logical record types (Type-1 through Type-16)
        - Type-1 Transaction record
        - Type-2 User-defined descriptive text record
        - Type-3 Low-resolution grayscale record
        - Type-4 High-resolution grayscale record
        - Type-5 Low-resolution binary record
        - Type-6 High-resolution binary record
        - Type-7 User-defined image record
        - Type-8 Signature image data record
        - Type-9 Minutiae record
        - Type-10 Facial & SMT (scar, mark, and tattoo) image record
        - Type-11 Record reserved for future use
        - Type-12 Record reserved for future use
        - Type-13 variable-resolution latent image record
        - Type-14 variable-resolution tenprint image record
        - Type-15 variable-resolution palmprint image record
        - Type-16 User-defined testing image record
    - Record Formats (ANSI/NIST-ITL 1-2000)

F. BIOMETRIC APPLICATION FLOW REQUIREMENTS

Biometric data must flow from those who are gathering the data and then into the BFC's huge database, ABIS, which processes it. This process can be done several different ways. The way this chapter will describe it is the way the USSOCOM-NPS

Cooperative Field Experimentation Program has been testing the network flow of fingerprints from a “suspect” or an “unknown individual.”

USSOCOM-NPS Cooperative Field Experimentation Program takes the suspects fingerprints, usually 10-print rolled, on the Cross Match device shown in Figure 15. This is a kit that was purchased by USSOCOM that was utilized by the BFC during the TNT exercises. It’s important to note that the BFC does not endorse any biometric product.

Figure 14. Cross Match jump kit the BFC uses per USSOCOM.

In the lower left corner of Figure 14 is the Cross Match #ID 442 R device which has the Live Scan capabilities that captures the image of fingerprints. It’s similar to the large Live Scanners used at Police Departments, only miniaturized. The ID 442 R is hardwire connected to the CF-18 Panasonic Toughbook laptop. The laptop has the Cross Match software installed on it, so when fingerprints are taken they are automatically displayed on the screen. The software will make a beep and display a still image of the prints if they are accepted by the software. Another way the Cross Match system displays acceptance or rejection of prints taken is if the corresponding little round lights

located to the left of the ID 442 R and above the blue rim of the scanner light up green for accept and red for reject (refer to Figure 14).

1. 10 – print Rolled Fingerprints

The process to gather 10-print rolled fingerprints is one where each individual finger print is not only placed flat, but rolled onto the Cross Match scanner. The fingers are placed on their side on top of the Cross Match scanner and then rolled across the scanner until they reach the opposite side. This insures that all of the data possible is collected from that fingerprint. This is the most complete way to obtain all the fingerprint data possible.

2. 10 – print Flat Fingerprints

10 print flat fingerprints actually consist of 2 "slaps," one from each hand that consists of the four fingers starting from the pinkie ending with the index. The right hand is placed on the Cross Match scanner first then the left. Then both of the thumbs are placed on the scanner and are captured. This is a quicker method of fingerprinting, but is necessarily not the best way. The current standards and industry prefer using 10-prints because more information is gathered. That's why the 10-print rolled is preferred because it allows for the sides of the fingers to be captured as well. The importance of this is explained in the Latent fingerprint section.

3. Latent Fingerprints

The current systems used to collect fingerprints are not sophisticated enough to capture a fingerprint that is left behind. Latent fingerprints are ones that are manually captured by a human from an object. It is a forensic scenario and the person capturing the fingerprints use a soft brush and powder (magnetic or florescent) or they could use a special adhesive tape. Rolled fingerprint information is very important, especially in a case of identifying latent fingerprints. For example, if there is a latent print that is being lifted from piece of debris that was from an IED, it might only be a partial print that is the side of a finger. This instance is where having a rolled fingerprint as opposed to a flat fingerprint in ABIS could make all the difference in identifying an IED maker.

G. STEPS OF THE CROSS MATCH APPLICATION

When gathering fingerprints while using the Cross match application, one must first fill out the steps that are listed in the flow chart below in Figure 15. Figures 16-23 show exactly the fields the must be filled out. Then the finger prints can be rolled and Figure 24 is the result. All the information is then sent to the ABIS database to see if there is an "ident," that is when someone has been enrolled previously and are in the system or if it is an "non ident" which is when there is no match.

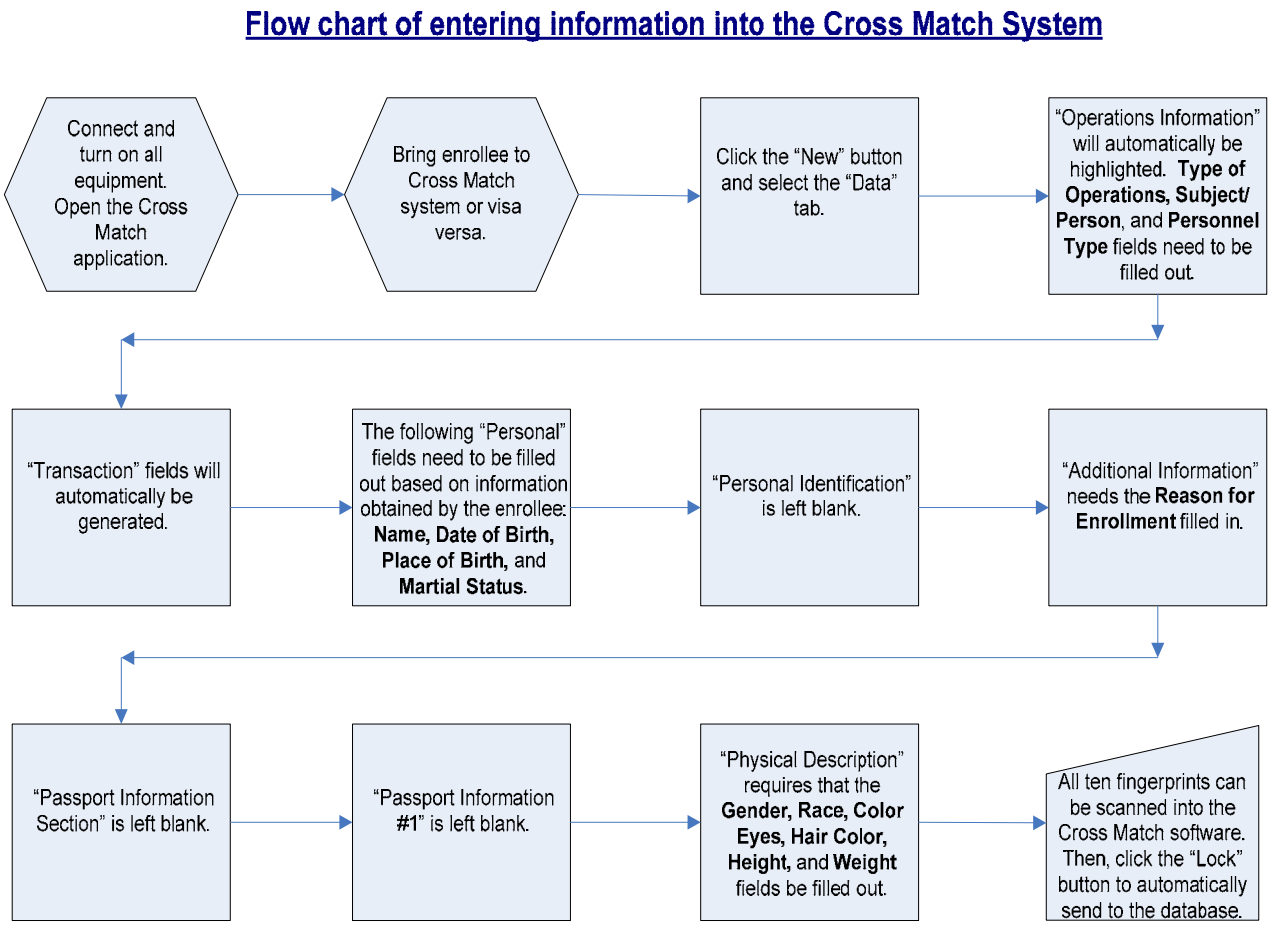

Figure 15. Flow chart of Cross Match process.

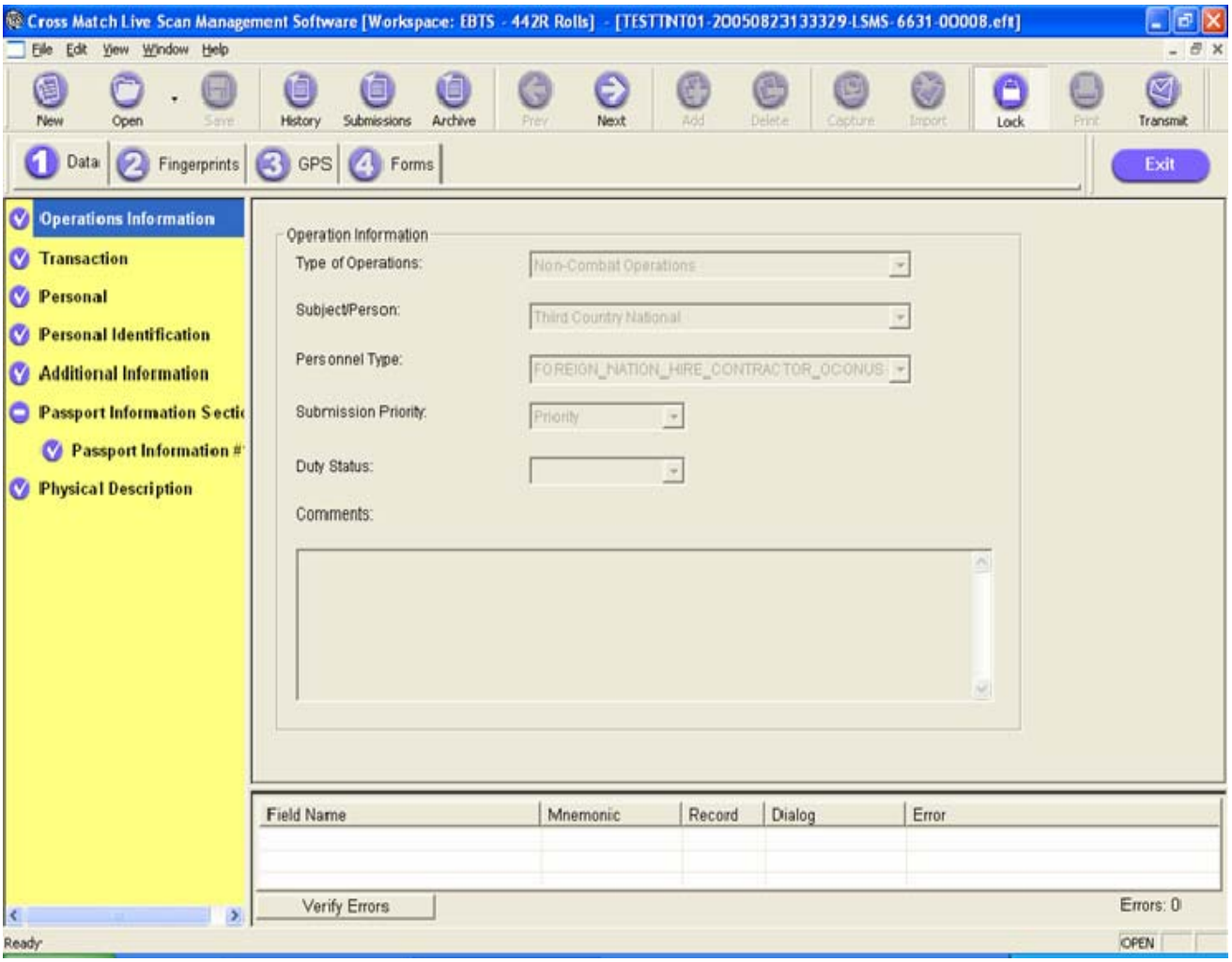

Figure 16. First Step – Operations Information (screen shot taken from personal use of Cross Match software during field experiments)

In the first step, the following fields needs to be filled out:

Type of operations

Subject/Person

Personnel Type

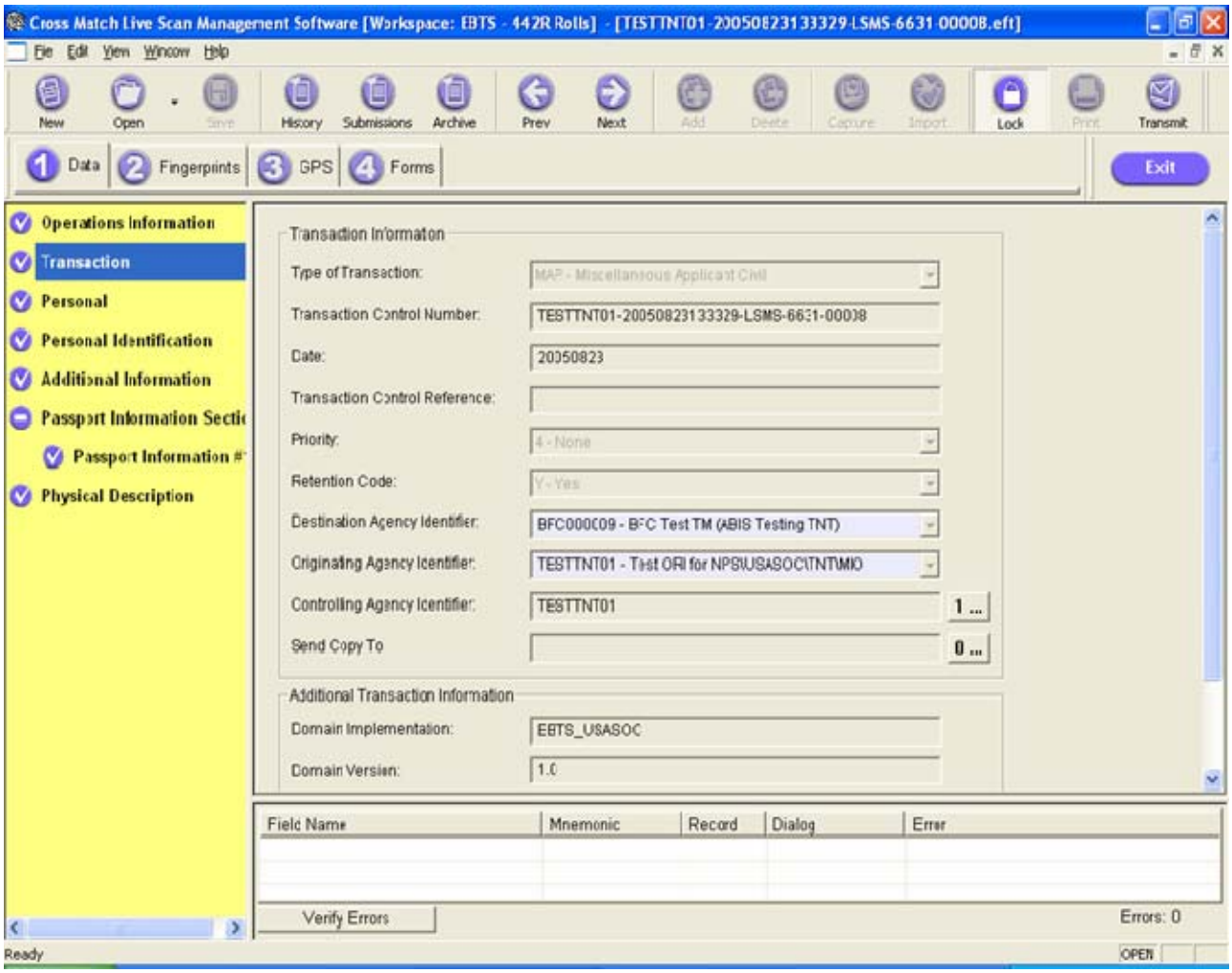

Figure 17. Second Step – Transaction (screen shot taken from personal use of Cross Match software during field experiments)

This step's information is automatically generated.

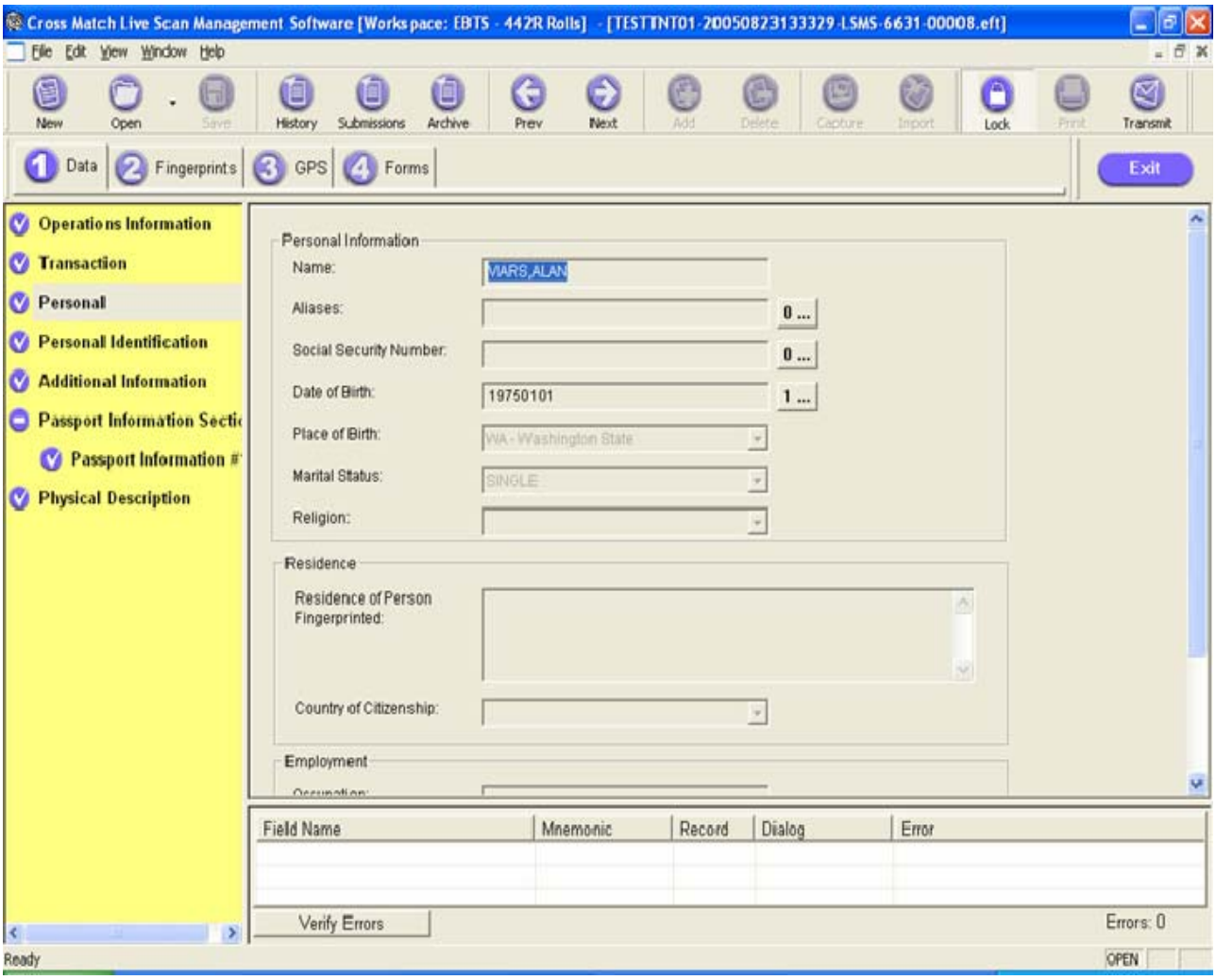

Figure 18. Third Step – Personal (screen shot taken from personal use of Cross Match software during field experiments)

Personal information is inputted. This is supposed to be obtained from the enrollee.

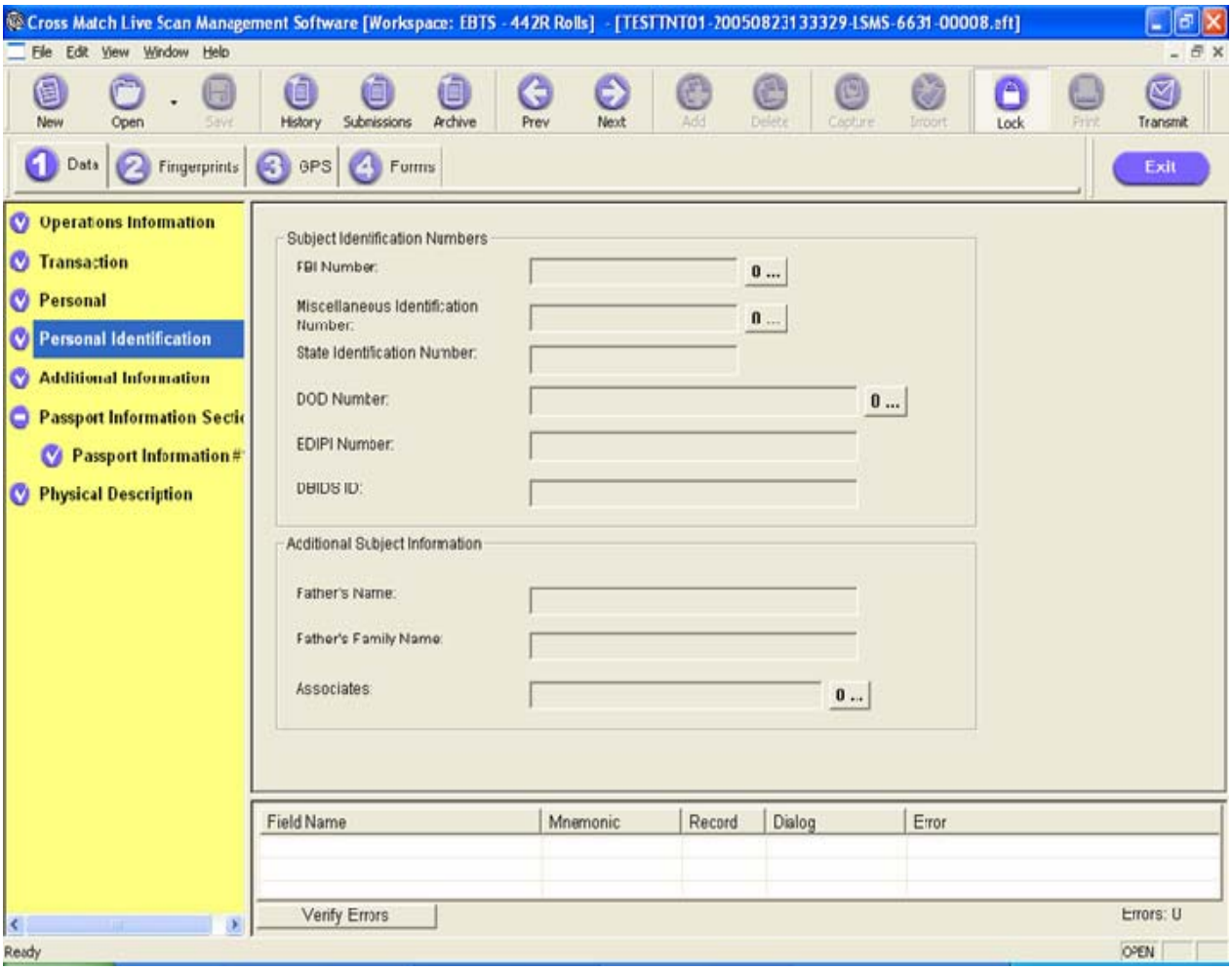

Figure 19. Fourth Step – Personal Identification (screen shot taken from personal use of Cross Match software during field experiments)

The Personal Identification screen is not necessary to fill out.

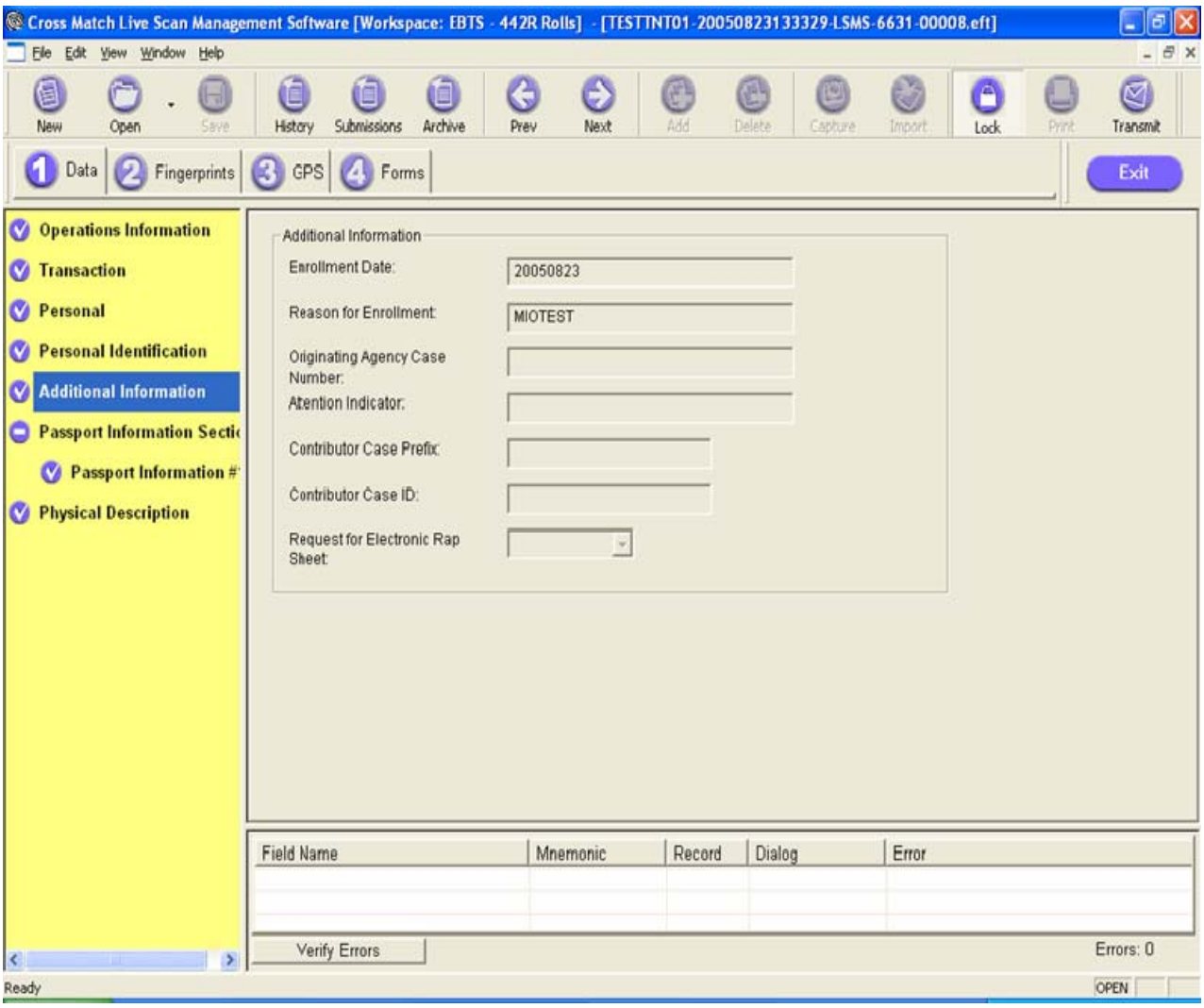

Figure 20. Fifth Step – Additional Information (screen shot taken from personal use of Cross Match software during field experiments)

The reason for enrollment must be filled in.

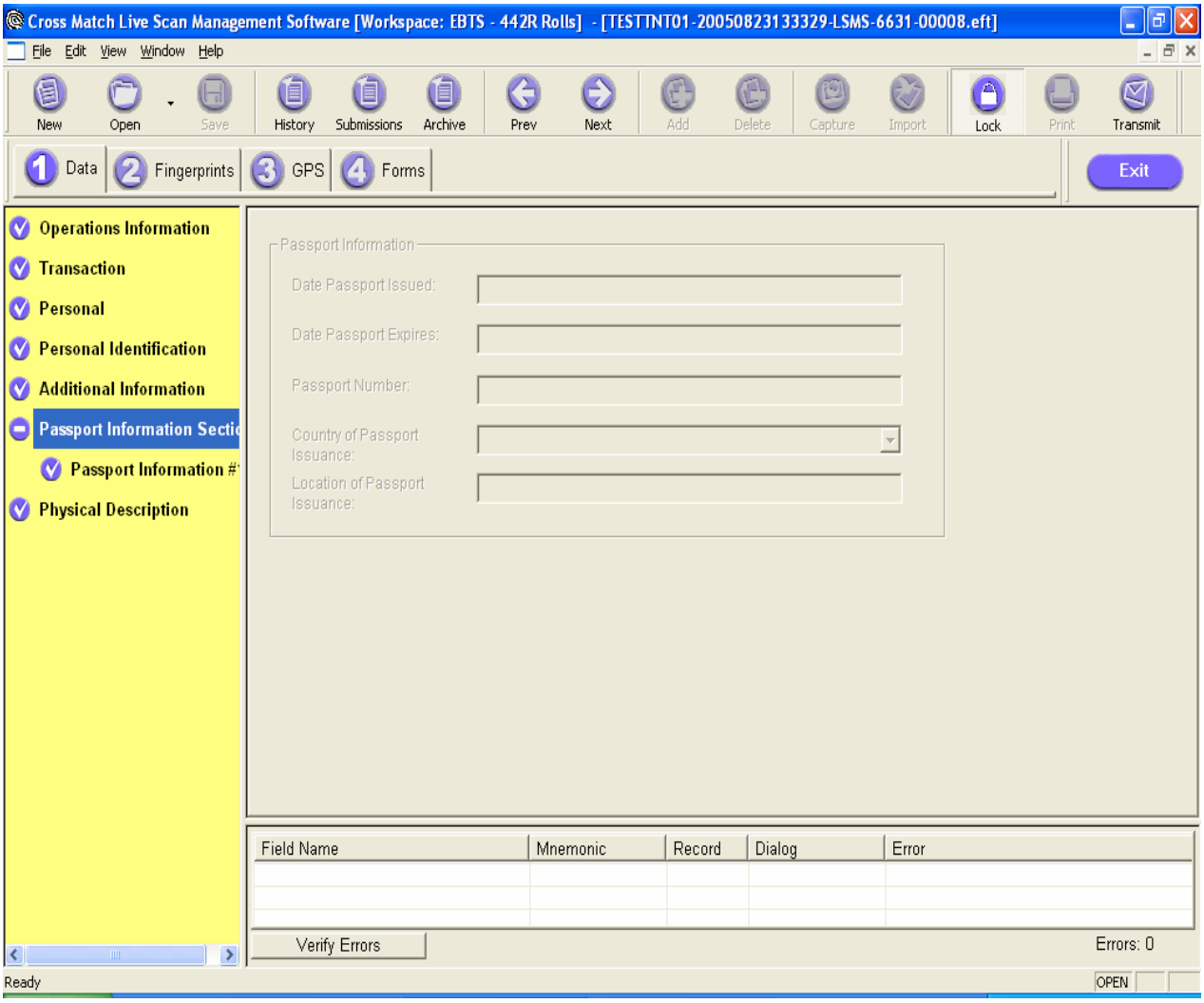

Figure 21. Sixth Step, Passport Information Section (screen shot taken from personal use of Cross Match software during field experiments)

Data does not need to be input into this section.

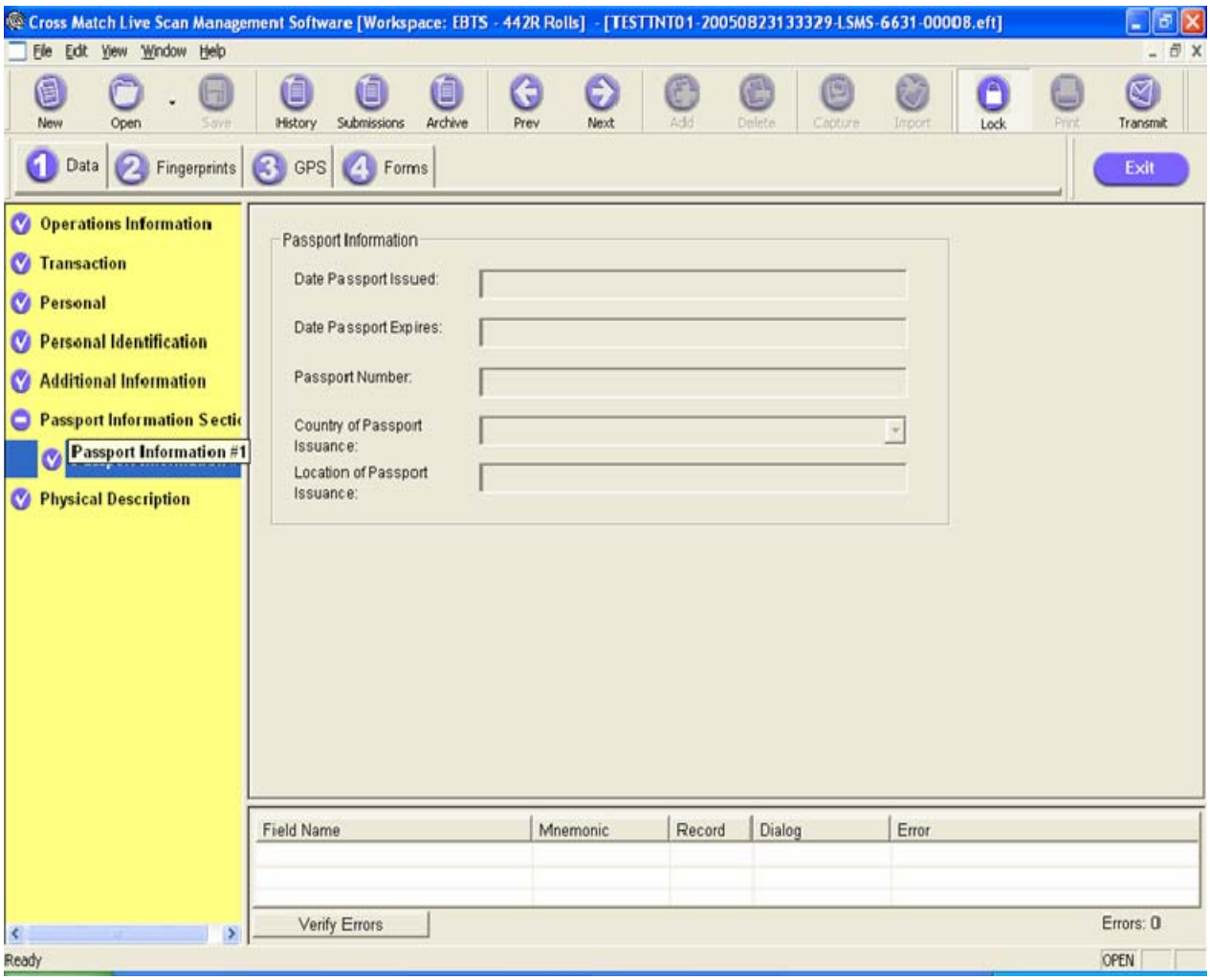

Figure 22. Seventh Step – Passport Information #1 (screen shot taken from personal use of Cross Match software during field experiments)

Data does not need to be input into this section.

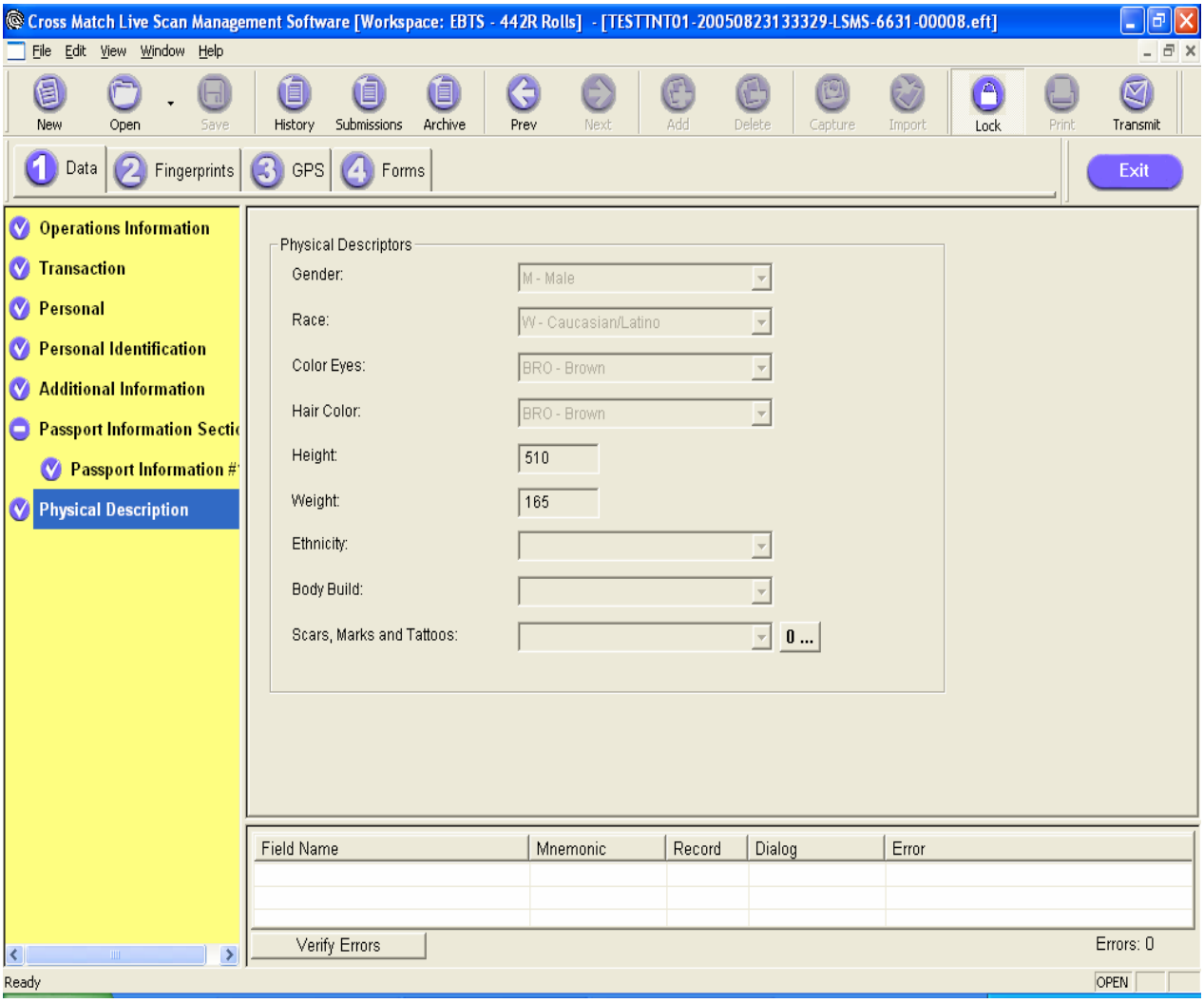

Figure 23. Eighth Step – Physical Description (screen shot taken from personal use of Cross Match software during field experiments)

The following fields must be filled out:

Gender

Race

Color Eyes

Hair Color

Height

Weight

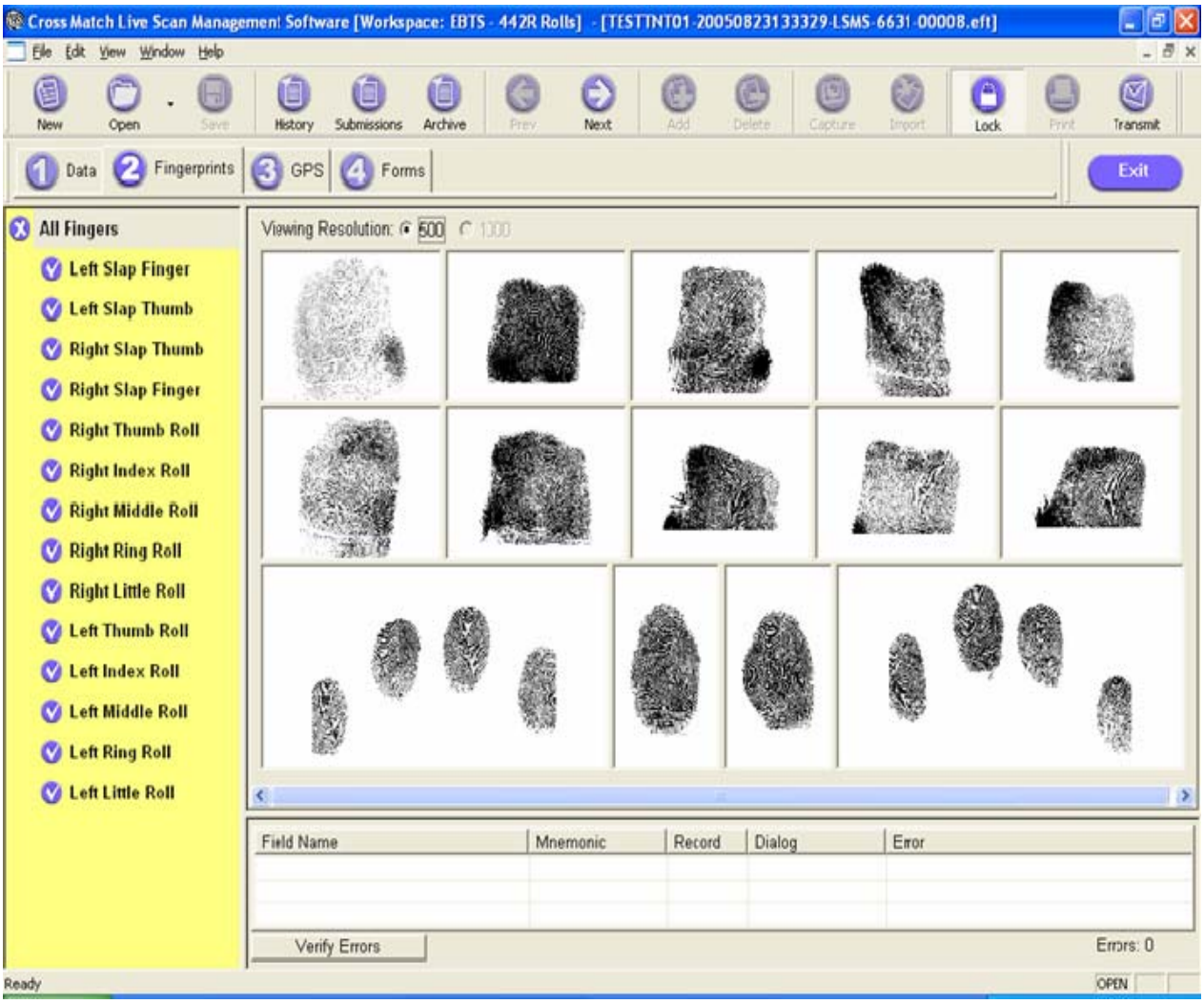

Figure 24. Ninth Step – Finger prints (screen shot taken from personal use of Cross Match software during field experiments)

All 10 fingerprints are enrolled using a scanner and then they are displayed digitally. At this time, all of the Figures are considered one file and can be sent to the database for processing.

H. BIOMETRIC MEASURES OF PERFORMANCE

There are many measures of performance (MOP) one could look at in the realm of biometrics. For instance the quality of sample taken, image resolution, correct count of minutiae, and many other criteria used in different ways to determine measures of performance of a device that one is using. The Biometrics Fusion Center tests and evaluates biometric systems for EBTS/EFTS compliance. The FBI certifies 10-print rolled biometric scanners for image quality. The MOP's that will be looked at are the ones that relate to the way that we used biometrics in the USSOCOM-NPS field experiments.

The time it takes to enroll a person is a critical element in a tactical situation. The device used is a deciding factor in this situation. If you are using a device that can only take one fingerprint at a time then the time to take a full set of ten-prints is greatly increased. If you are able to take the "slaps" of the four fingers and then the two thumbs together, then your time is reduced, but the sides of the fingers are not captured. Currently, there is no solution to have both speed and completeness, one must decide what is more valuable for their situation.

An important measure of performance for the experiments, because it directly translates to what would happen in real life, is the delay of transmission of the fingerprints. Rapid identification verification of an unknown person is crucial in a real life situation. The soldiers on the ground do not want to be waiting around for very long if they have a hostile suspect they are trying to control or if they are in a vulnerable spot that could be attacked. Time is of the essence in the tactical environment. This is when the network that the solider has available to him is of the utmost importance. The crux is the time it takes to reach back to the ABIS database.

Another measure of performance is once the data has arrived via the network to ABIS database, how long does it take to have the fingerprints processed? The time it takes to determine if there is a positive identification or non-identification is valuable, and therefore must be as short as possible. Once the fingerprints have been processed, then the results will need to be sent back to the solider who is waiting for the response.

I. CONCLUSIONS

Besides there being biometric standards there are networking and operational standards that need to be considered. Using the correct network in different situations is key to how quickly one can get a response from the ABIS database. Considering the environment in which the finger printing is taking place also plays an important role. For instance, CONOPS for biometric identification in a tactical network is not known. The next chapter explores how using the USSOCOM-Naval Postgraduate School Field Experimentation Program provides the unique capability for evaluating the biometric identification process requirements in emerging tactical networks.

V. RESULTS FROM THE FIELD EXPERIMENTS

In August of 2005 the USSOCOM-NPS Cooperative Field Experimentation Program started experimenting with the use of Biometric Fusion Center's products. The BFC has participated in every experiment since then. They usually bring their Cross Match #ID 442 R system to use during the scenarios. At the beginning of each of the following sections will be a brief description of that iteration's scenario, this is because they vary and change each time. A high value target (HVT) or a person of suspicion or interest is who the BFC is looking for within the TNT scenarios. The steps of conducting the BFC's work are acquiring the biometric identifiers, transmitting, matching and then returning the results of biometric identifiers.

A. TNT 05-4

1. Camp Roberts (August 29-2 September 2005)

Part of the premise for the August 2005, TNT 05-4 scenario was a High Value Target (HVT) search in 3 buildings located in the Camp Roberts facility. A dismounted team of soldiers, the "ODA team" equipped with a picture of the HVT, Tacticomps, 3 HMMWV's, and an LRV, entered into each building and secured it. Per the script written for this scenario, one building was found completely empty. The second building did not have any HVTs but did reveal WMD (weapons of mass destruction) and IED (improvised explosive device) materials. The "ODA team" secured the materials and left a surveillance camera and proceeded to building three. The last building did contain one HVT. Once the "ODA team" confirmed that the HVT was the same as the in their picture, they brought him outside and processed him for fingerprints. Several questions were asked in order to complete the data input required for what was a one gigabit file once the rolled 10-prints were taken.

The scenario was conducted twice, each time using a different network to send the information back the BFC for processing. August 30, 2005 was scheduled for the first run of the scenario with the use of Iridium Satellite, but was delayed until the next day. The reason for the delay was that Hurricane Katrina Relief efforts had priority in the Iridium Satellite system and all other users lost their service. In light of this the scenario was slightly modified and instead of using Iridium for reachback, other technologies were

utilized. On August 30, 2005, 3 tethered balloons with ITT Mesh provided primary communications between the LRV and TOC (in place of Iridium). On August 31, the Iridium services were restored and utilized.

High Value Target Identification was accomplished by first posting the biometrics sensor data output in the Groove workspace, shared by LRV, TOC, NPS NOC, and Biometrics Fusion Center (DoD BFC). DoD BFC could open that file out of the shared workspace that was being connected by Verizon or Iridium to the TOC, then a VPN connection from the NPS NOC to DoD BFC. Once the BFC received that data, they processed it. Biometrics identification data, (seen below) was returned into the shared workspace from DoD BFC:

> Ident for 00025.eft
>
> ---
>
> WVBFC0001
>
> TCN: WVBFC0001-200508301934-TNTT-DMDC-00001
>
> ECN: 20050320000000007199
>
> NAME: ZEDNAN,ALJAZERA
>
> ABIS#: 000138087 DATE RECEIVED: 20050826
>
> SEX RACE BIRTH DATE HEIGHT WEIGHT EYES HAIR
>
> M W 1963/09/24 510 160 BN BN
>
> ARRESTED OR RECEIVED: 20050320
>
> CHARGE: SUSPECT OF IED CELL
>
> LOCATION: OLDSMAR, FLORIDA (TNT 05-4 AAR, p.6)

As discussed above, HVT biometric data was transmitted from the field to the TOC two ways. The first way used an Iridium network, which reflects current capabilities. Processing this information via Iridium took at least 70 minutes. 70 minutes is a time threshold that exceeds what most soldiers are willing to wait. The second form of transmission was an advanced network using the ITT mesh and the LRV. The ITT mesh network required 12 minutes for results to reach the operator (TNT 05-4 AAR, p. iii) Examining the difference of times (12 minutes versus 70 minutes to complete this task) demonstrates that the type of network can have a great impact on the speed of field operations (TNT 05-4 AAR, p.6)

2. Monterey Bay (August 22-25, 2005)

This was an exercise of capabilities that could be used during a Maritime Interdiction Operation (MIO) experiment. It was conducted in the Monterey Bay using wireless 802.16 as a reachback from the ship-to-shore, from the shore to the NPS NOC, and from the NOC to the BFC via a VPN. The USCG HAWKSBILL cutter was used as the ship being boarded by the NPS, BFC, and Lawrence Livermore National Laboratory (LLNL) teams. The purpose of the exercise was to provide boarding parties with near-real time feedback of biometric screening and radiation detection\signatures on a boarded vessel. Below is a section taken from LT Marvin's thesis, because it best explains the sequence of events that took place:

> To be tested was the Man-Pack OFDM backhaul link, LLNL Ultra-Wideband (UWB) interface and portable biometrics gathering equipment.
>
> Network availability was provided by the 802.16/OFDM backbone from the Beach Lab, and Man-Pack 802.16/OFDM to Biometrics, UWB, video, and Radiation detection devices.
>
> Network availability and capability was then tested throughout the boarding evolution conducted on USS HAWKSBILL.
>
> Network availability was tested to the most remote node (UWB) and Man-Pack 802.16/OFDM throughout the boarding evolution to determine the effects of bulkhead and deck penetration of UWB and backhaul distance from HAWKSBILL to CYPRESS SEA effect on the OFDM link.
>
> **EVENT 1**
>
> NPS Man-Pack, LLNL UWB, Biometrics Fusion Team, and IST development teams boarded the USS HAWKSBILL. UWB, Boarding Officer, and Radiation detection, and Biometrics teams established and stabilized boarding team LAN on target vessel. Man-Pack Operator established OFDM link to CYPRESS SEA and sent audio/video link via Groove workspace to collaborative partners.
>
> **EVENT 2**
>
> Biometrics fusion team established connectivity and began gathering and processing biometrics from suspect vessel crew via reach back to the Biometrics Fusion Center provided by TNT test-bed.

EVENT 3

After OFDM link was established, LLNL team interfaced UWB with the OFDM link and streamed video back to the NOC.

EVENT 4

LLNL team used a portable radiation detector to evaluate potential cargo of interest onboard USS HAWKSBILL. Radiation data was streamed through the OFDM backbone and associated portal to LLNL remote technical assistance engineers for identification.

EVENT 5

While boarding teams were aboard HAWKSBILL the IST development team observed and documented ergonomic and functional requirements for future under-development portable radiation detection and source identification units. (Marvin, p.53)

The MIO exercise tested collaborative software, situational awareness tools, wireless 802.16 technology, including the mobile 802.16, the Man-Pack, radiation detection, UWB, and biometrics. All parties involved in the operational exercise communicated in a virtual workspace, called Groove. LLNL detected radiation and communicated within the ship using ultra wideband technology. Ultra wideband is a low frequency, broad band technology that can penetrate through a ship's haul or through steel containers. Using Groove, the BFC provided near real-time, automatic biometric feedback on those persons encountered during operational exercise. Timing between the boat and the BFC was never actually measured because this was the first initial test of feasibility. The main question was "is it possible to send biometrics from a target ship?" The answer was yes, but timing at this point was not a MOP.

B. TNT 06-1

In November 2005 the first experiment of the 2006 fiscal year was conducted.

1. Camp Roberts (November 12-18, 2005):

Below is a description of the two scenarios that were accomplished.

Scenario # 1a and #1b

Operators were conducting routine check point (CP) operations when a suspicious individual tried to cross the bridge into the controlled area. UAVs were providing surveillance and security flights in the vicinity of the bridge. The individual was taken

under control and moved to a secure holding area to the side of the bridge. A picture of the individual was sent to the Tactical Operations Center (TOC). A 10-print method of biometrics ID was utilized. The forward deployed (FD) CP operators had a laptop that had the ability to input this biometric data. They also had a Transaction Manager Viewer laptop.

The 10-print data were sent via the TNT network to the BFC. Two variations of the TNT network were evaluated. The first (Scenario #1a) had the Light Reconnaissance Vehicle (LRV) located on a hill ~300 meters from the CP. The LRV had line-of-site (LOS) to the CP and to the TOC. ITT mesh was the comms between the CP and LRV. Then from the LRV to TOC, high throughput 802.16 was used. Scenario #1b imitated the possibility that the LRV may not be able to obtain LOS to both the CP and TOC. So instead, a tethered balloon was raised to provide the ITT mesh network communications between the CP and the TOC. Rather than have the LRV as comms node, there was an end-to-end ITT mesh network (TNT 06-1 Scenarios, p.2).

Scenarios #2a and #2b

Through human intelligence sources, the TOC learned that an important Al Qaeda leader will make his way over the bridge to attend a meeting. The TOC asked for this vehicle to be identified and marked with a tag if possible while it is on the bridge. While the target vehicle waited in line on the bridge, operators placed a tag on it. The TOC airboss decided to put the longer endurance Tern UAV in the air and directed it to take a picture of the vehicle and to maintain Surveillance and Reconnaissance (S&R) and to determine any potential meeting location. Once the threat vehicle passed through the CP it evaded the Tern's S&R. TOC directed appropriate UAVs (Raven, Pointer, Tern, NPS SUAV) to conduct simultaneous search missions in the most likely areas. Once located, the "ODA team" proceeded to the vehicle and observed from distance that driver had departed. Vehicle then became a potential IED. Some UAVs were re-tasked to search for the high value target (HVT) in the vicinity of vehicle and provided S&R of possible IED vehicle. Once a UAV located the HVT on foot, TOC directed the "ODA team" to that location so that they would take the HVT under control. The operators took a ten-print and facial picture from the HVT. The fingerprint data was sent for ID as in Scenarios #1. The facial image was sent to the TOC. Once the operators received

positive ID, they moved back to the TOC with the HVT and the mission was completed. Meanwhile, the UAVs were assisting in determining the status of the IED and its disposal. (TNT 06-1 Scenarios, p.2)

These scenarios were made feasible by using collaborative tools. Groove was used for collaboration between UAV operators at local and remote sites and for collaboration of the LRV with the BFC. VPN between the BFC and Camp Roberts was established and functioned properly. (TNT 06-1 AAR, p.5)

Ten-prints were sent from the field to the BFC Automated Biometrics Identification System (ABIS) emulator (the operational ABIS was not used) through a hardware enabled VPN. Using a hardware VPN concentrator at the BFC allowed access to several BFC servers with different databases needed for biometrics identification (TNT 06-1 AAR, p.7-8). Figure 25 pictorially dictates the network flow diagram for biometrics sharing. We successfully demonstrated advanced HVT Identification from the field by transmitting a ten fingerprint file to the Biometrics Fusion Center and receiving a proper identification match in 6 minutes (TNT 06-1 AAR, p.ii).

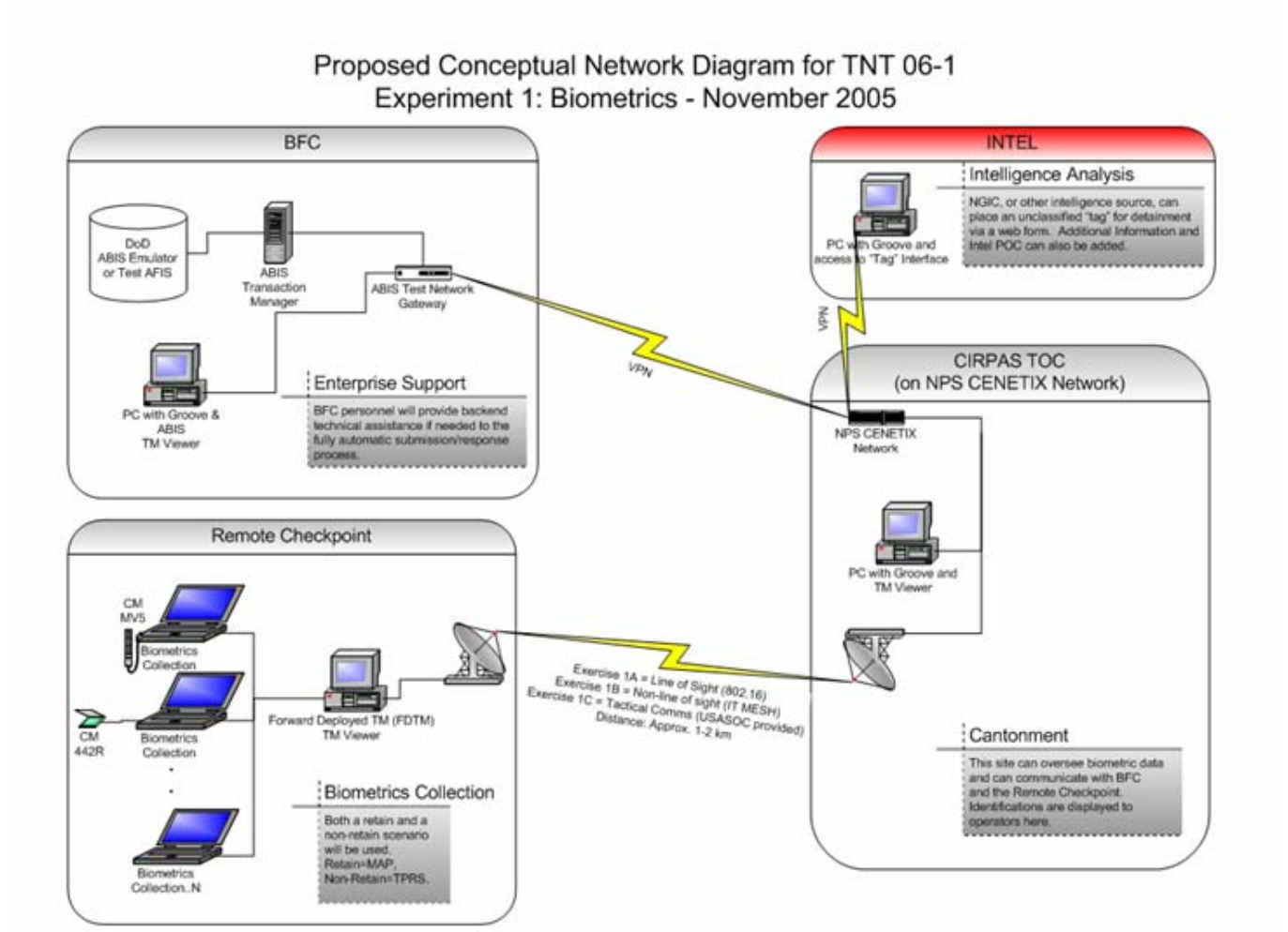

Figure 25. Biometric Network Flow Diagram for TNT 06-1 (Provided by Viars, BFC)

2. San Francisco/Alameda Island MIO (November 20-22 2005)

The basic scenario for this experiment was drafted by Dr. Bordetsky and the following is a synopsis: After gathering intelligence and authorizations of both US and Country X Governments, the USCG has ordered one of its cutters to stop, board, and search a vessel suspected of transporting uranium enriching equipment and explosives from Country Y to a terrorist cell. In trying to locate uranium enriching equipment and explosives, and while minimizing disruption to Country X's main port, the USCG Operations Center, Alameda has directed its cutter to employ radiation detection, explosives detection, and biometric equipment to expedite the at-sea search. Since positive identification of the source in a short time is imperative, a wireless network

extension capability was to be extended from the cutter to the boarding team. That network reached back to LLNL and the Defense Threat Reduction Agency (DTRA) to assist in identification of suspect cargo. Support from the DoD Biometrics Fusion Center must be used to quickly and accurately discriminate between actual vessel crewmembers and non-crew suspects (TNT 06-1 MIO, p3).

Docked ships at the MARAD (Maritime Administration) station on Alameda Island were used to simulate at-sea conditons. One was a crane ship, called the GEM State and one was a cargo vessel ship named the Admiral W.M. Callaghan. GEM State was the simulated USCG Cutter and the Admiral W.M Callaghan was the boarded ship with suspect cargo and personnel.

The objectives of this experiment were to continue to test the ability of a Boarding Party to rapidly set-up ship-to-ship communications that allow it to search for radiation and explosive sources and identify personnel while keeping in contact with the originating ship and so that remote collaboration with sensor experts can be possible.

The schedule of events was as follows:

Event 1

OFDM link was established between USCG Headquarters, Alameda and the support ship GEM STATE.

Event 2

Boarding team (to include Boarding Officer, Assistant Boarding Officer with networks expertise and 802.16/OFDM Man-Pack radio, LLNL UWB and Radiation Sensor teams, and Biometrics Collection Team) boarded the ADMIRAL CALLAHAN and set up 802.16/OFDM network extension to the GEM STATE. LLNL and Biometrics Collection Teams began setting up and stabilizing a LAN with the Boarding Officer. Event 2 was complete when the LAN and link between the ADMIRAL CALLAHAN and the GEM STATW was operational.

Event 3

Biometrics fusion team began gathering and sending biometrics from the suspect vessel's crew to the Biometrics Fusion Center via network (TNT test-bed VPN). The Biometrics Fusion Center evaluated the biometrics data and sent their analysis information to the boarding officer via the same network.

Event 4

Radiation detection team with portable radiation detectors evaluated suspect cargo and began sending radiation detection information from their location via the network (UWB-to-OFDM backbone-to-VPN portal) to LLNL for technical analysis. Streaming Video data was also sent to LLNL and DTRA for analysis support. The Boarding Officer collaborated over Groove with higher headquarters (USCG Headquarters, Alameda) and Centers of Excellence (LLNL, BFC, and DTRA) to support analysis and situational awareness of all organizations.

Event 5

While boarding teams were aboard the ADMIRAL CALLAHAN, the LLNL team observed and documented ergonomic and functional requirements for future development of portable radiation detection and source identification units.

Event 6

Retrograde from ADMIRAL CALLAHAN and GEM STATE and USCG Headquarters, Alameda occurred. Pre-experiment conditions at each location were restored. Appropriate check out was conducted with supporting organizations. (TNT 06-1 MIO, p3).

The results from TNT 06-1 MIO scenario were successful. An advanced ship-to-ship communication network capability was setup within 15 minutes. Because of this, both biometric and radiation detection data were quickly and accurately transmitted to the BFC and Lawrence Livermore National Laboratory. The response time for biometrics data sharing and response from the BFC was reduced to 4 min. (TNT 06-1 AAR, p.10)

C. TNT 06-2

TNT 06-2 was conducted in the second quarter FY 06; in Monterey, CA from 20-24 February at Camp Roberts, CA from 27 February-3 March 2006, and in Alameda, CA from 5-7 March 2006. The Monterey portion that was carried out during 20-24 February did not contain biometrics.

1. Camp Roberts (27 February - 3 March 2006)

The main scenario which BFC participated in was a scenario of a red force passing through a checkpoint and blue team trying to identify them. The scenario simulated operations that were occurring in several locations at different times in which biometrics and INTEL were collected. Data mining and analysis, provided by Brandes

Assoc. RMITS, were utilized to identify that there was a threat of HVTs. A convoy was deployed to man a checkpoint. The CP had biometrics for ID of personnel (BFC ten-prints and BFC latent print extraction). Six UAVs were simultaneously utilized in an air-space-deconflicted, optimized search to locate the HVTs. Each operating area had an ITT Mesh cluster which was linked through the 802.16 long-haul backbone to the TOC using mobile TOCs (i.e. NPS LRV). The TOC was linked to multiple remote sites including the BFC (Clarksburg, WVa), USFS (Missoula, MT) via VPN, and to Avon Park, FL via SATCOM/VPN.

There were capabilities shown for biometrics collection and data transmission that were dramatic. The results of this scenario showed that the ten-print files were collected and sent from the field to the BFC with a response obtained in an average of four minutes. Figure 26 shows the flow of biometrics during this experiment. This scenario also called for the demonstration of latent print lift capability. Prints were collected by a professional latent lifter and then sent to the BFC database, evaluated, and a response received within 30 minutes. BFC had very positive results using their Automated Biometrics Identification Systems (ABIS) Emulator ten-print record matching capability. (TNT 06-2 AAR, p2)

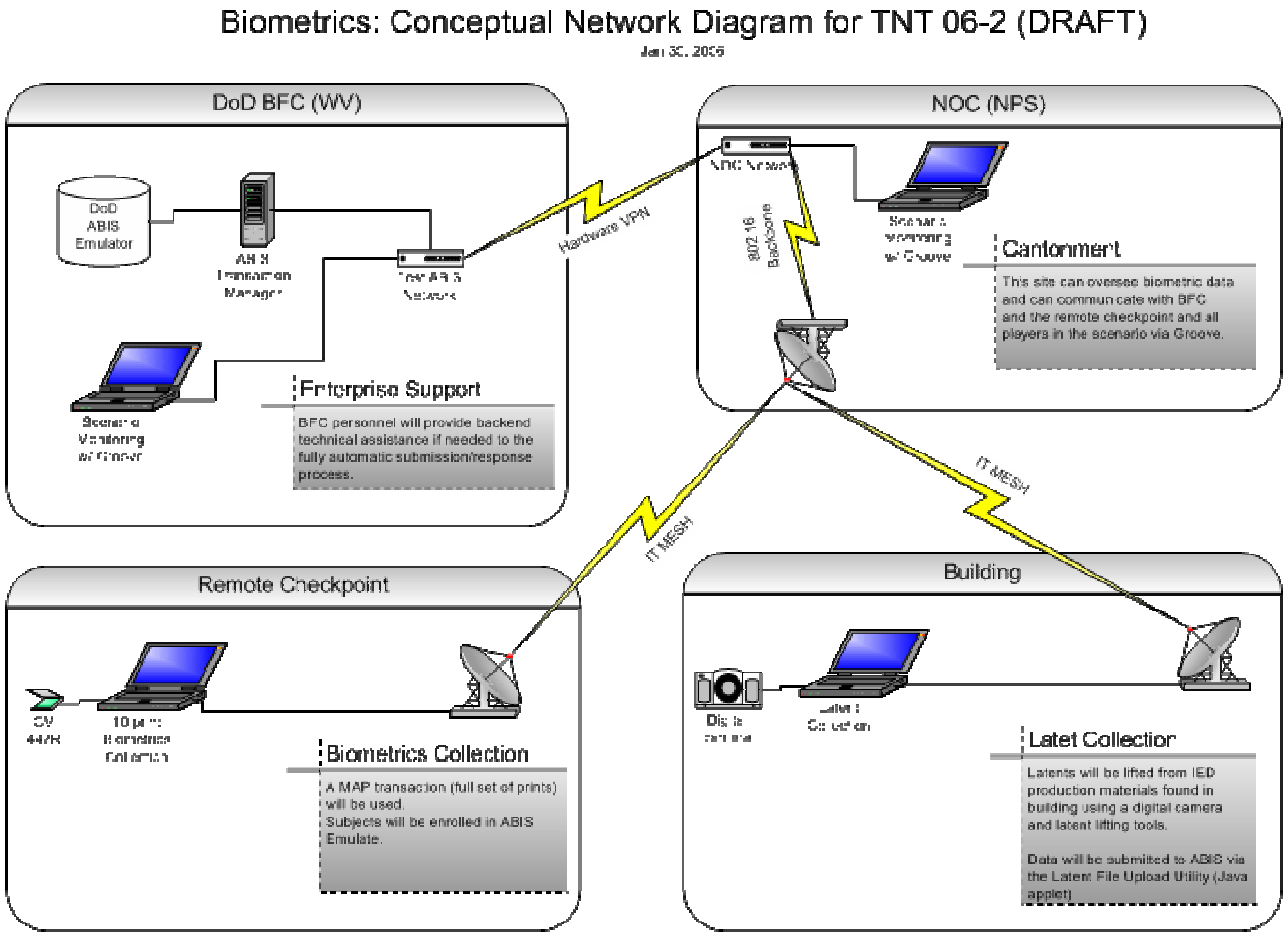

Figure 26. Biometric Network Flow Diagram for TNT 06-2 (Provided by Viars, BFC)

2. San Francisco MIO (March 5-7, 2006)

The scenario of TNT 06-2 for Maritime Interdiction Operations portion of the experiments strived to be a real life scenario that is fundamental to all agencies and institutions involved in homeland security operations, specifically, those related to maritime interdiction.

> According to intelligence, a cargo vessel that departed country X in early February was carrying a terrorist cell with hazardous (radiological) material and was attempting to enter the country via a West coast port. The Vessel's name and port of arrival are unknown.
>
> Multiple boarding operations are ongoing (and updates are posting to Maritime Intelligence Fusion Center - MIFC via E-Wall). Intel provided updated information and gave high confidence that a vessel entering

Washington State had the terrorists onboard. USCG and NSWC decided to coordinate the vessel's takedown.

Under that course of action, USCG ordered one of its vessels (simulated by MARAD SS Gem State) to stop, board, and search a ship (simulated by USCG Cutter, called the Tern) suspected of transporting radiological material as well as a terrorist cell. In order to do that, while the suspect vessel is underway, a RHIB with a boarding team was employed.

Level I boarding team conducted a search of the vessel due to its status as a high interest vessel (HIV). They were equipped with radioactive detectors. During the inspection, a neutron alarm was triggered on a radioactive detector. The alarm was a constant alarm, not spurious counts. The Level I team called in a Level II team to resurvey the ship with their additional radiation detection equipment.

So, in order to assist in locating suspects, uranium enriching equipment and explosives, the USCG Operations Center, Alameda directed its Level II boarding team to employ radiation detection, explosives detection, and biometric equipment to help expedite this at-sea search. Since there are numerous commercial uses for certain radioactive sources and positive identification of the source in a short time is imperative, a network extension capability was utilized from the suspect vessel to the boarding team's launch vessel and ashore. This rapidly deployable, collaborative network reached back to LLNL and the Defense Threat Reduction Agency (DTRA) to assist in identification of suspect cargo. Support from the Biometrics Fusion Center must be used to quickly and accurately discriminate between actual vessel crewmembers and non-crew suspects.

The tasking for Level II boarding team was to conduct a survey of the cargo ship and identify the source of the neutron readings. Also, using biometrics recording devices, crew members must take fingerprints and that biometrics data had to be to BFC for identification.

The expected boarding scenario events were:

- Hidden neutron source in engine room and hidden gamma source as cargo. BFC fingerprints Captain and crew.

- First gamma spectrum of gamma source taken is poorly done because the boarding party took too short of a spectrum. Reachback can ask for second spectrum for analysis. Gamma spectrum of neutron source and photos sent to reachback and export control for identification.

- Once the identification of the items is passed to the boarding team and fed to MIFC, the cognitive process clock starts where the

experts work in collaboration with MIFC and USCG support vessel to understand the situation and come up with a course of action to deal with the threat.

- Once the captain of the ship is located, he can inform the boarding party that he had a soil density gauge that emitted neutrons (but only after we send spectra and photos of item). Export control should identify it as soil density gauge. Unfortunately, it was stolen. The captain can't explain the gamma source- possible terrorist threat? Captain's fingerprints show him to be on a watch list.

The radiological material was simulated by detection files that provided the LLNL analysis team with some ambiguity about the severity of the material. Once that determination was passed to the boarding team and fed to MIFC, the cognitive process clock started where the experts work in collaboration with MIFC, USCG and boarding team to understand the situation and come up with a course of action to deal with the threat. (TNT 06-2 MIO)

The team was able to carry out the scenario with success and received viable results for all concerned. Biometrics was able to identify the crew members and the key was to keep the biometric exchange flowing while the target boat was on the move utilizing 802.16 and 802.20.

D. TNT 06-3

1. Camp Roberts (June 3-9, 2006)

The main scenario for TNT 06-3 was: "Force-on-Force". There was a blue force, which consisted of multiple types of UAS's, TOC, etc. who's goal was to find the red force, which in turn consisted of 3 SORSE (special operations research and support element) soldiers on ATV's (all terrain vehicles). The scenario started at 1300 and lasted until 0100, so that both EO and IR cameras could be tested. The red team was instructed to stay above a 35 degrees and 45 minutes line, north of the TOC until 1800. At that point they were allowed to penetrate closer to the TOC. During a predetermined time of the scenario, the red team would (purposefully) cross through a checkpoint and be fingerprinted. The BFC local database (in the TOC), called the Mobile Automated Fingerprint Identification System (MAFIS) was used to match the fingerprints against a list of about 100 people that had been downloaded from ABIS. A response was generated by the local database at the TOC. Two 'Hit' and one 'No Hit' responses were

received by the enrollment unit because only two members of the red team were previously enrolled for the scenario. Results for the matching took only 2 minutes. See Figure 27 for the biometric data flow.

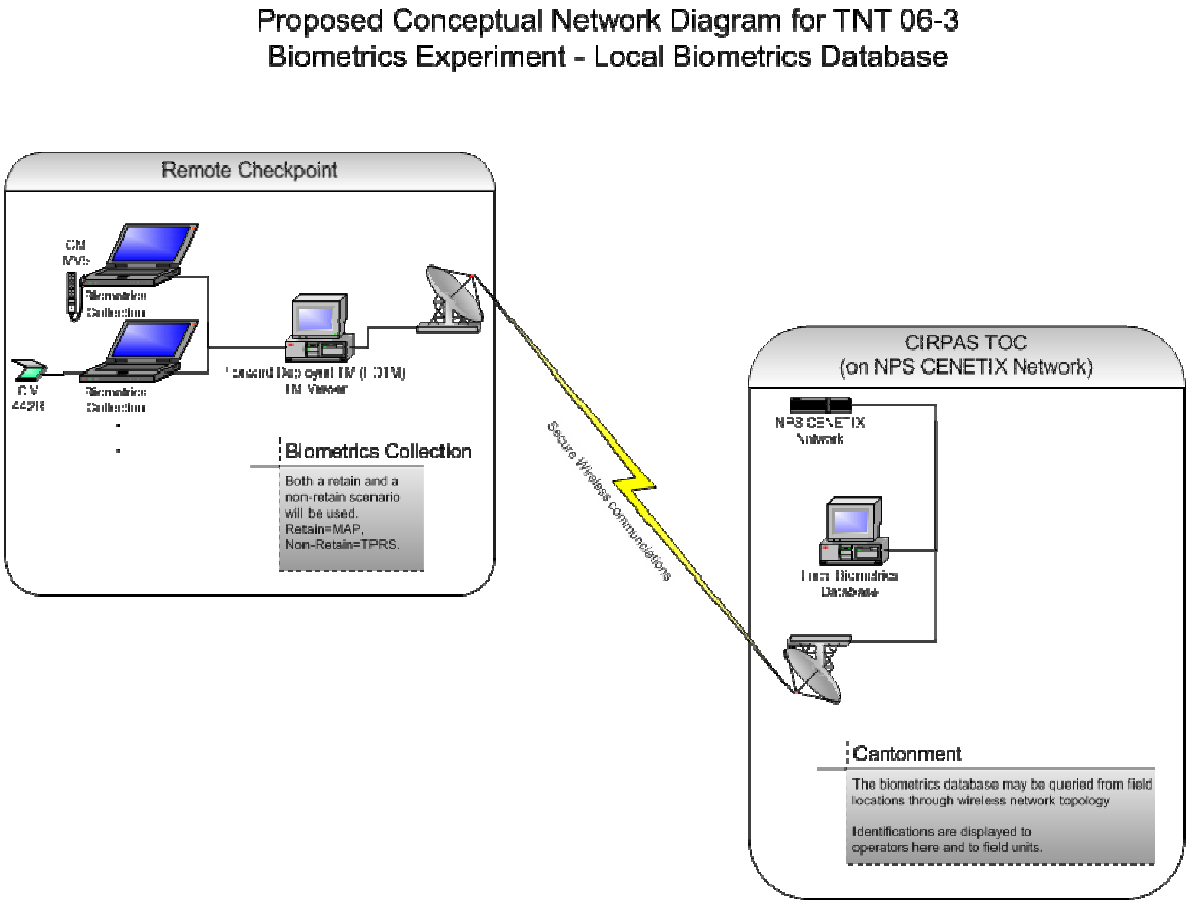

Figure 27. Biometric Network Flow Diagram for TNT 06-3 (Provided by Viars, BFC)

2. San Francisco MIO (June 13-15, 2006)

The scenario for the MIO portion of TNT 06-3 was very similar to those in the past. Below is narrative of the background of the scenario:

> A month ago, an Austrian border facility's sensor detected a radiological source, but the alarm failed to activate and the truck was able to continue on without being searched. It apparently delivered its cargo to a port on the Baltic Sea. There were several ships in port at that time. It was reported that a truck of similar type loaded cargo on a vessel of Swedish Registry. Once the sensor malfunction was uncovered, the Swedish Authorities were notified and subsequently conducted a search of the suspect vessel. That search found no radiological material. A list of ships

> in the port in the time frame of the shipment was developed. One ship was headed to the Caribbean with several stops and finally to a Mexican port. Arrangements were made to search the vessel when it arrived in the Mexican port. No sources of radiation were found on the ship. The Austrian's provided the sensor data to the Swedes; the data is troublesome in that it indicates a possible Pu source as there was both gammas and neutrons measured. The Austrian's and Swedes have (scenario assumption) an agreement which authorizes a collaborative effort between their country's (military/law enforcement) teams to continue to determine what the source was and ensure that appropriate action is taken with respect to it (TNT 06-3 MIO).

Based on this background, intelligence reports were received that indicated a cargo vessel was carrying a hazardous (radiological) material. The vessel and its cargo are attempting to enter the country via a West Coast port. The United States Coast Guard decided to conduct a Maritime Interdiction Operation. After boarding the vessel, the search team located a hidden neutron source in the engine room and finds a hidden gamma source onboard as cargo. Fingerprints were taken of the captain and crew. The response file was supposed to have returned from the captain's fingerprint file showing that he has an outstanding warrant. Prior to the experiment starting, the captain's fingerprints were loaded as a print that was to be identified as a suspect. Unfortunately, the prints were not properly loaded, and therefore all prints taken during experiment came back as "No Hit." Biometrics personnel enrolled and submitted the fingerprints to Biometrics MAFIS Computer, located in TOC, via the 802.16 connection between the boarded vessel and the TOC. Biometrics MAFIS computer automatically replied, within 2 minutes. Biometrics personnel also took three sets of prints, via Biometrics Enrollment laptop, and files were made available to Biometrics MAFIS computer at TOC. Biometrics MAFIS provided "No Hits" on watch list for all three prints.

The following should be noted regarding this experiment:

> The current database used in this experiment only held less than 100 people and only matched right indexes. The outstanding warrant enrollee was not identified during the experiment. For testing purposes, the enrollee's fingerprints were captured again. The file was matched only to the print that was captured during the scenario. This error could be the result of poor fingerprints, an incorrectly connected fingerprint matching license key, or possibly the limited 'right index' search capability (TNT 06-3 AAR – BFC).

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND RECOMMENDATIONS

There were several measures of performance that were looked at. One of them was the completeness of the fingerprint taken. For most of the experiments a device that could accommodate rolling the finger from side to side was used. That was the most complete amount of information that could be taken of ones' fingerprint. In TNT 06-3 a smaller device that only took flat (not rolled) fingerprints was taken and therefore there was less information, but it was completed in less time, because only the two thumbs and two index fingers were gathered.

One of the main measures of performance that was evaluated was the length of time that it took to transmit the fingerprint data from the field back to the ABIS database. Although this was not measured in every experiment, there was a range of times and during each subsequent experiment there were quicker turn around times. The longest time that was observed was 70 minutes (using low bandwidth Satellite communications), while the shortest time was 4 minutes for reachback to ABIS and 2 minutes for a local database. Lifting latent fingerprints and sending them took a grand total of 30 minutes to retrieve a response. Please see Figure 28 for brief summary of the type of networks used and times of for responses for each event.

Another MOP was the network environment that was in place in order to conduct and run a full set of prints. There are key components used in the network. For example was it wired or wireless? How far is the network being stretched? Is it going through a satellite, a VPN, or is it local? All of these could factor into how long it takes or if one can process fingerprints.

One also needs to take into account the applications used. Is Cross Match being used to gather the data or another application? What kind of method is being used to send the information back to the database? Is it being sent via Groove or file transfer? All of these factors can make a difference.

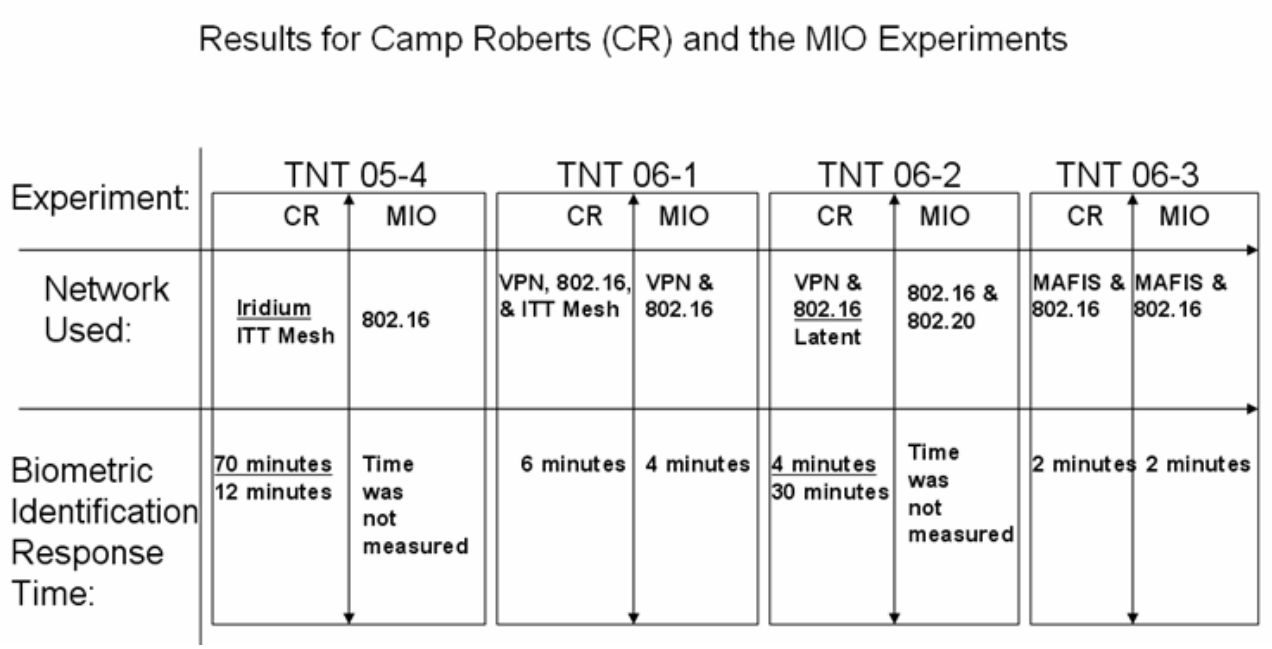

Figure 28. Evolution of Biometrics Identification Performance through TNT Experiments

The USSOCOM-NPS Cooperative Field Experimentation Program proved that biometrics is feasible at the tactical level, while having remote access with the BFC. The times to obtain identification were primarily due to the megabit size file that was being transmitted. In the last experiment the time required was as little as 2-4 minutes.

One must keep in mind that because the fingerprint files are large (~1 megabit), they do require either very large bandwidth or significant time to transmit. Communications robustness and speed will be critical if the identification cannot be made on-site with a local database. The current policy is off-site identification and off-site links to related intelligence matches. Quick identifications based on limited data sets may be done at forward areas without transmitting real-time (TNT 06-1 AAR, p.7-8).

Fingerprint acquisition tools are somewhat large for full tactical use, and require minutes to collect valid prints. This may be insufficient in some environments. The form factor could be made smaller and more portable. If these issues were looked at and improved, then the warfighter might be willing to include this technology in their already overloaded required gear as shown in Figure 1. Utilizing multiple biometric measures may actually result in shorter transmit and database search times.

This thesis modeled and structured the process of biometric identification in a testbed environment. It showed that the biometric process was improved through each consecutive experiment. It is these improvements which lead to operationally viable results of receiving biometric response within minutes. This thesis concludes that this technology has great potential for fighting the war on terrorism and warrants continued studies. Possible areas of future research are: smaller/portable devices, local databases or "watch lists", optimal networks for reachback to ABIS, emerging reliable biometrics, different biometric modalities (especially facial recognition).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Analyzing. *Analyzing Images of Human Faces*. Last accessed in March 2006 from http://www.cs.cmu.edu/afs/cs/user/tk/www/Projects_www/IU_white_paper/face/davis_face.html

ANSI/NIST-ITL 1-2000. 2000. *American National Standard for Information Systems – Data Format for the interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information.* http://sequoyah.nist.gov/pub/nist_internal_reports/sp500-245-a16.pdf

BFC. *What we do*. Last Accessed on July 20, 2006 from http://www.biometrics.dod.mil/Content/content.aspx?NavID=4

BFC Standards. *Biometric Standards*. Last Accessed on July 20, 2006 from

http://www.biometrics.dod.mil/Content/Content.aspx?NavID=4&PageID=181

EBTS ver1.1. 2005. *Department of Defense Eelctronic Biometric Transmission Specification*. Last accessed in April 2006 from

http://www.biometrics.dod.mil/documents/DoD_ABIS_EBTS.pdf

Facial. *Facial Features Identification*. Last Accessed on March 18, 2006 from http://et.wcu.edu/aidc/BioWebPages/Biometrics_Face.html

Identification. *Identification versus Verification*. Last Accessed on November 15, 2006 from http://www.findbiometrics.com/Pages/guide4.htm

Iris. *Iris and Retina Identification.* Last Accessed on March 18, 2006 from http://et.wcu.edu/aidc/BioWebPages/Biometrics_Eye.html

Iris Recognition. 2000. *Iris Recognition at airports uses Eye-Catching Technology*. Last Accessed in March 2006 from

http://archives.cnn.com/2000/TECH/computing/07/24/iris.explainer/

Keystroke. *Keystroke Dynamics Identification*. Last Accessed on March 19, 2006 from http://et.wcu.edu/aidc/BioWebPages/Biometrics_Keystroke.html

Layman's 2005. *A Layman's Glossary Of Biometric Terms*. Last Accessed on March 18, 2006 from http://www.biometricwatch.com/Glossary/glossary.htm

Manuel, C. E., Murphy, H. R. Jr., & Paxton, K. A. 2004. The Surveillance and Target Acquisition Network (STAN). (Master's Thesis, Naval Postgraduate School, Monterey, CA)

Marvin, Chris. 2005. 802.16 OFDM Rapidly Deployed Network for Near-Real-Time Collaboration of Expert Services in Maritime Security Operations. (Master's Thesis, Naval Postgraduate School, Monterey, CA)

Overview. 2005. *DoD Automated Biometric Identification System, DoD Electronic Biometric Transmission Specification Version 1.0 – Overview*. Last accessed in April 2006 from http://www.biometrics.dod.mil/Documents/DoD_ABIS_EBTS_Overview.pdf'

Patterns. *Fingerprint Pattern Types.* Last Accessed in March 2006 from http://www.fbi.gov/hq/cjisd/takingfps.html

Polemi, Despina. 1997. *Biometric Techniques: Review and Evaluations of Biometric Techniques for Identification and Authentication, including an Appraisal of the Areas Where They are Most Applicable*.pdf

Signature. *Signature Identification*. Last Accessed on March 19, 2006 from http://et.wcu.edu/aidc/BioWebPages/Biometrics_Signature.html

STAN 6 Brief. 2004. Last accessed in November 2006 from http://isgiant.nps.navy.mil/ussocom/STAN_6/STAN%20Brief.pdf.

TNT 05-1 Brief. 2004. Last accessed in November 2006 from http://isgiant.nps.navy.mil/ussocom/TNT_05-1/1_TNT-STAN05Brief.pdf

TNT 05-4 AAR. 2005. *U.S. Special Operations Command/Naval Postgraduate School Cooperative Field Experimentation Program, Tactical Network Topologies 05-04, After Action Report.* Last accessed in November 2006 from http://isgiant.nps.navy.mil/ussocom/TNT_05-4/TNT%2005-4%20AAR%20Final.pdf

TNT 05-4 Scenario. 2005. *SOF HVT Search with Convoy IED Threat – Scenarios 2-3a and 2-3b.* Last accessed in November 2006 from http://isgiant.nps.navy.mil/ussocom/TNT_05-4/Scenario2-3ab.pdf

TNT 06-1 AAR. 2005. *U.S. Special Operations Command/Naval Postgraduate School Cooperative Field Experimentation Program, Tactical Network Topologies 06-01, After Action Report.* Last accessed in November 2006 from *http://isgiant.nps.navy.mil/ussocom/TNT_06-1_AAR.doc*

TNT 06-1 MIO. 2005. *Scenario: connectivity and Collaboration for Radiation Awareness, Biometrics Fusion, and Maritime Interdiction Operations*. Last accessed in November 2006 from

http://isgiant.nps.navy.mil/ussocom/TNT_06-1AL/BoardingScenario.doc

TNT 06-1 Scenarios. 2005. *TNT 06-1: UAV Airpspace Deconfliction during SOF Operations*. Last accessed in November 2006 from http://isgiant.nps.navy.mil/ussocom/TNT_06-1CR/scenarios.doc

TNT 06-2 AAR. 2006. *USSOCOM/NPS Field Experimentation Program, Tactical Network Topologies 06-02 After Action Report.*. Last accessed in November 2006 from http://isgiant.nps.navy.mil/ussocom/TNT_06-2_AAR.doc

TNT 06-2 MIO. 2006. *Ship-to-Ship and Ship-to-Shore 802.16 links used for Maritime Interdiction Operations.* Last accessed in November 2006 from

http://isgiant.nps.navy.mil/ussocom/TNT_06-2AL/TNT_MIO_draft.doc

TNT 06-3 AAR. 2006. *USSOCOM/NPS Field Experimentation Program, Tactical Network Topologies 06-03 After Action Report*. Last accessed in November 2006 from http://isgiant.nps.navy.mil/ussocom/TNT_06-3_AAR.pdf

TNT 06-3 AAR – BFC. 2006. Last accessed in November 2006 from http://isgiant.nps.navy.mil/ussocom/TNT_06-3/BFC%20AAR.doc

TNT 06-3 MIO. 2006. *Joint USSOCOM-NPS-LLNL Field Experimentation Augmented by OSD/HD MDA Programs*. Last accessed in November 2006 from http://isgiant.nps.navy.mil/ussocom/TNT_06-3AL/TNT06-3_MIO_PLAN_-6_JPL-ab.doc

Verification. Verification (1:1) vs. Identification (1:N)**.** Last Accessed on November 15, 2006 from http://www.zvetcobiometrics.com/Support/biometrics_101/verification_identification.html

Voice. *Voice Identification.* Last Accessed on March 19, 2006 from http://et.wcu.edu/aidc/BioWebPages/Biometrics_Voice.html

Wang, Y., Tan, T., & Jain, A. 2003. Combining Face and Iris Biometrics for Identity Verification. Last Accessed in April 2006 from http://www.springerlink.com/content/pvvqf8we6qjfrauu/fulltext.pdf,

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Alex Bordetsky
   Naval Postgraduate School
   Monterey, California

4. Dr. Dave Netzer
   Naval Postgraduate School
   Monterey, California

5. Dr. Dan Boger
   Naval Postgraduate School
   Monterey, California

6. Ms. Marianna Verett
   Naval Postgraduate School
   Monterey, California

7. Mrs. Kim Woods
   Biometrics Fusion Center
   Clarksburg, West Virginia