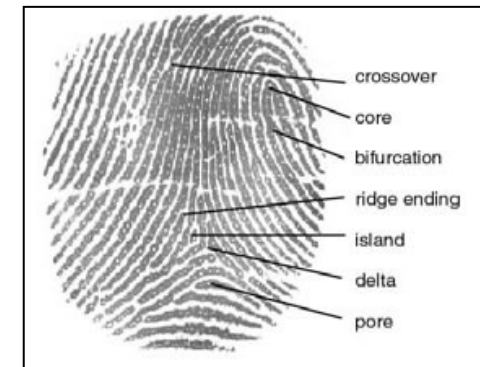# DoD Biometrics

NDIA
Disruptive Technologies

5 Sep 2007

Mr Tom Dee
Director, Defense Biometrics
OSD AT&L, DDR&E
thomas..dee@osd.mil (osd.smil.mil)
703-746-1385

crossover
core
bifurcation
ridge ending
island
delta
pore

Outline

- **The Problem**

- **Traditional Solutions**

- **Disruptive Technology**

- **DoD Biometrics**

Friend? Enemy? Neutral?

Combat Identification

"Combat Identification is the process of attaining an accurate characterization of detected objects in the battle space to the extent that a high confidence, timely application of tactical options, and weapons resources can occur. Depending on the situation and the tactical decisions that must be made, this characterization will be at least, but may not be limited to, "friend," "enemy," or "neutral." Combat identification functions encompass cooperative and non-cooperative identification capabilities."

Joint Pub 3-01, 5 Feb 2007
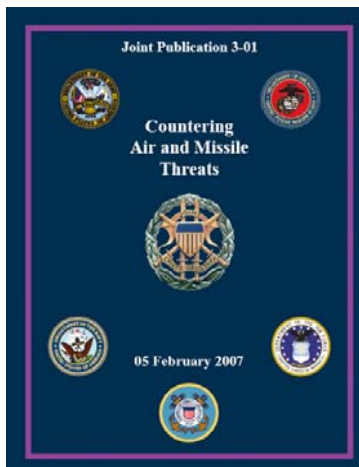
Combat Identification

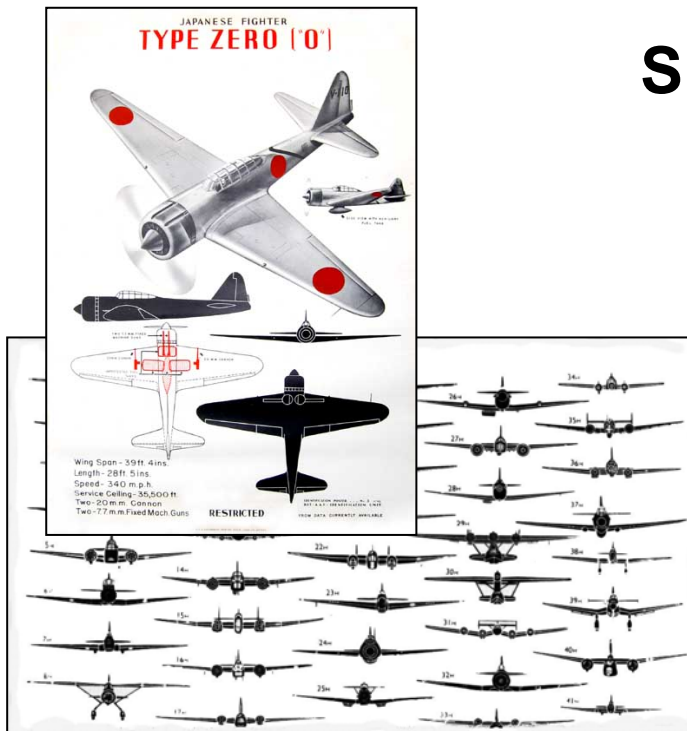- **How to classify and identify detected objects?**

Shapes?

People

Platforms

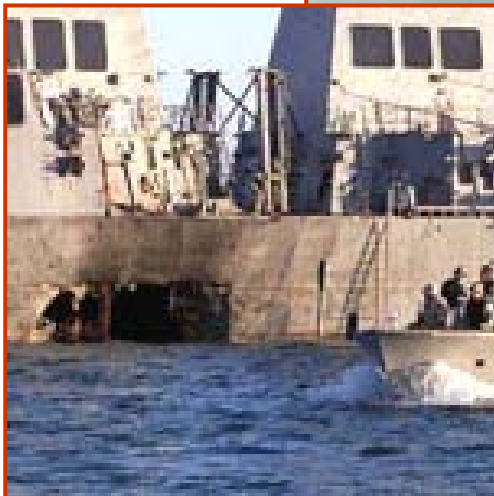**Markings?**

Signatures?

Signals?

What if the "object" is a non-state actor?

Enemy?

Neutral?

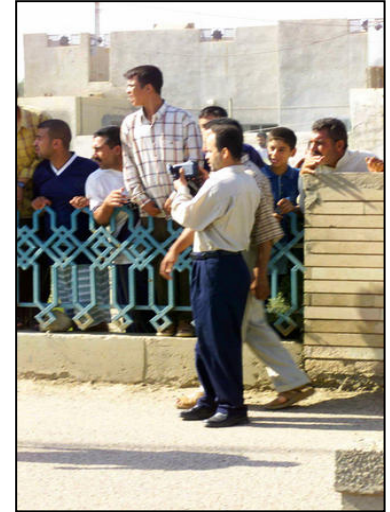**Friend?**

Classification

• **Tactical decisions require:**

- **Detection**

- **Classification**

Airspace control integrates different airspace users and provides them with responsive and timely support.

• **But, how do you classify an anonymous individual?**

- **Something he's wearing?**

- **Something he's carrying?**

- **His behavior**

- **His identity**
  - **Who he is**
  - **Where he's been**
  - **Who's he associated with**
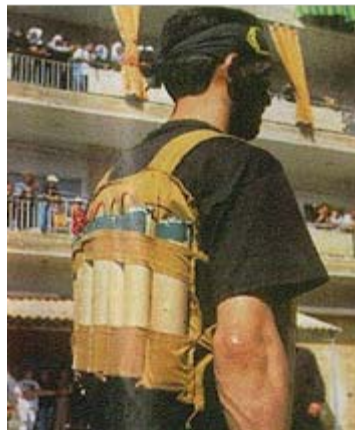
**Post IED Blast
AR RAMADI, IRAQ Jun 04**

**Reuters Video photographer
Unclassified**

6

And… What If You Get It Wrong

- **Consequences**
  - **Tactical**
  - **Operational**
  - **Strategic**

USS Cole

Friendly Fire
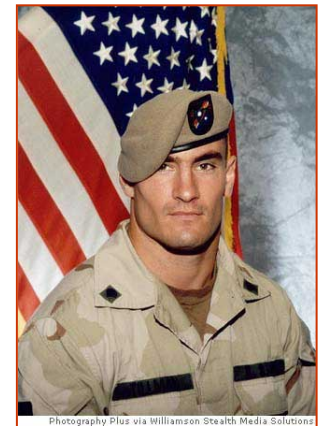
9-11

Iran Air 655

U.S. Bomb Dropped; 3 British Soldiers Die
NY Times, 25 Aug 2007

Traditional Solutions

Perimeter Systems

Alert
Zone

Exclusion
Zone

Situational Awareness
Zone10-15 km
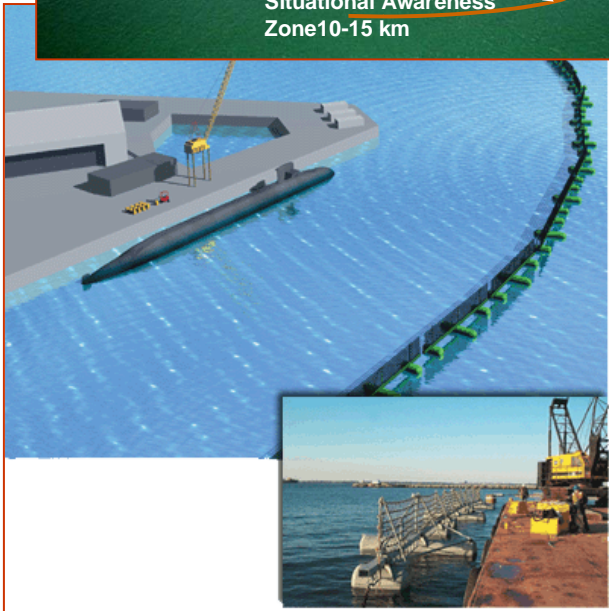
Deterrence

Detection technology

8

The Disruptive ID Technology

Stealth, Columbia Pictures, 2005

Terms of Reference

Biometrics – Biometrics are measurable physical characteristics or personal behavioral traits used to recognize the identity, or verify the claimed identity, of an individual.

Verification – a <u>one-to-one</u> matching process

Am I who I claim to be?

Identification – a <u>one-to-many</u> matching process

Who am I?

Why Biometrics in DoD?

In today's Joint Operating Environment "an anonymous enemy individual can be a tactical, operational, and even strategic threat."
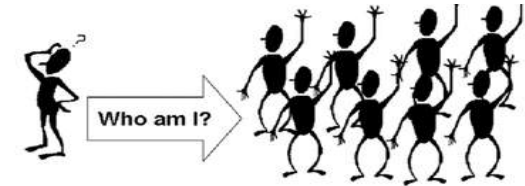
- **Business Functions**
  - **Physical and logical access controls**
  - **Privilege management**
    - **Health care, benefits, finance, time and attendance, etc.**

- **Military operations**
  - **"Combat Identification"**
    - **Friend, Foe, Neutral?**
  - **Offensive Operations**
    - **Intelligence support to targeting**
  - **Force Protection**
    - **Base access**
  - **Detention Operations**
  - **Civil-Military Operations**
    - **Track target members of population.**
  - **Personnel Recovery and identification**

Friend / Enemy / Neutral ?
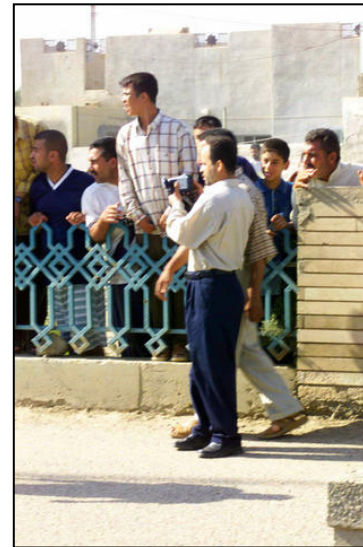
- **Confidence level of ID?**
- **Consequences of a wrong ID?**
- **Operational situation?**
- **ROE?**

**Post IED Blast
AR RAMADI, IRAQ Jun 04**

Reuters Video photographer

DoD Use of Biometrics

COLLECTION

1

▪ **ENROLLED IN BAT ON 18 SEP 05,** SUSPECTED SMALL ARMS FIRE

• **LATENT PRINTS RECOVERED FROM IED MATERIALS**

2

MATCHING & STORAGE

3,7

DOD ABIS CLARKSBURG WV

6 **25-JUL-07** Additional latent prints from same materials searched in ABIS

Enrolled in BAT on 9 JUL 07 due to capture as a result of Tier 1 alert in HIIDE

INTEL EXPLOITATION

4

NGIC PRODUCES BIAR LATENT MATCH NOTIFICATION 12 NOV 06 & 14 DEC 06

ACTIONS

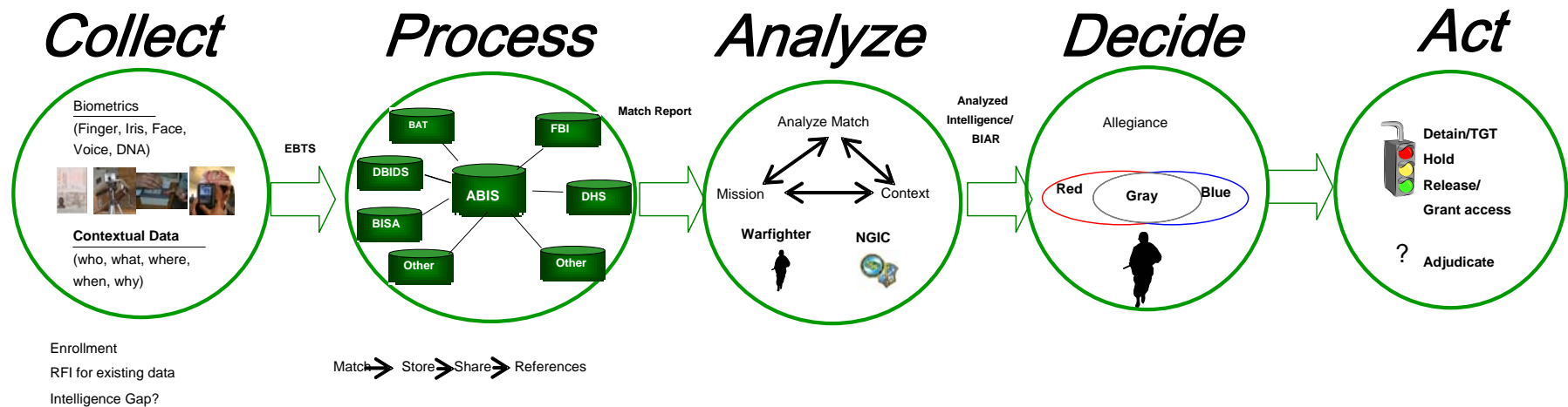**PLACED ON BIOMETRICS WATCHLIST, TIER 1 (DETAIN IF ENCOUNTERED)**

29 MAY 07 RECORD FLAGGED IN ABIS AND ALERTED IN BAT

5

CAPTURED 26 JUN 07 during Screening via HIIDE

Supporting Requirements

| Collect | Process | Analyze | Decide | Act |

Collect:
- Biometrics (Finger, Iris, Face, Voice, DNA)
- Contextual Data (who, what, where, when, why)
- Enrollment
- RFI for existing data
- Intelligence Gap?

EBTS

Process:
- BAT
- FBI
- DBIDS
- ABIS
- DHS
- BISA
- Other
- Other
- Match Report
- Match, Store, Share, References

Analyze:
- Analyze Match
- Mission, Context
- Warfighter, NGIC

Analyzed Intelligence/ BIAR

Decide:
- Allegiance
- Red, Gray, Blue

Act:
- Detain/TGT
- Hold
- Release/ Grant access
- ? Adjudicate

- **Sensors to collect**
- **Databases to store**
  - **Data to match**
    - **Biometric forensics**
- **Applications to process**
- **Communications to share**
- **Analysis tools for decision support**
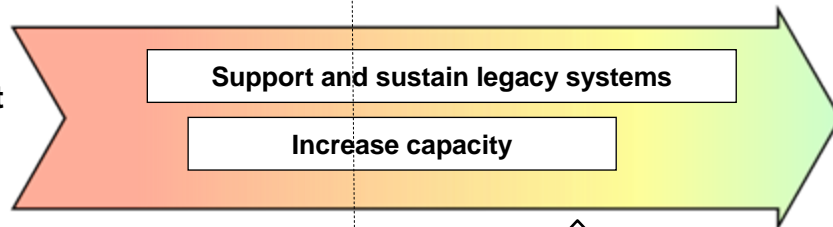
Biometrically Enabled Systems In Theater

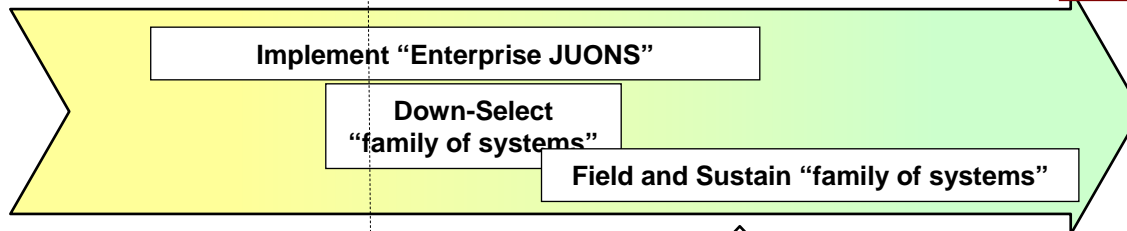| Source	Description	Biometric Type
Biometrics Automated Toolset (BAT)	Enemy combatants, detainees, locally employed personnel (LEP), misc. fingerprinted by the U.S. military; used for intel functions, LEP processing, detention mgt	Various Flat or Rolled Fingerprint, Photo, & Iris
Biometric Identification System for Access (BISA)	Base Access System where biometrics are collected from persons requiring access to U.S. installations in Iraqi; issues biometrically-enabled badge as credential	Ten Rolled Fingerprint, Photo, & Iris
Multi-Purpose Access Card (MPAC)	Iraqi applying for a position of trust or privilege with Iraqi Gov't; some stations are being use for criminal processing	Ten Rolled Fingerprint, Photo, Iris, & Voice
Expanded Maritime Interception Operation (eMIO)	Deployed on Navy patrols performing interception and boarding operations on the high seas	Ten Flat or Rolled Fingerprint, Photo, & Iris
Special Operations Command (SOCOM) Jump Kits	Deployed with SOF troops on tactical missions.	Various Flat or Rolled Fingerprint, Photo, & Iris
Detainee Reporting Systems (DRS)	Detainee Management, collecting biometrics from all detainees held for more than 14 days and assigned an ISN number; Red Cross-compliant	Ten Rolled Fingerprint & Photo
Defense Biometric Identification System (DBIDS)	Base access system; collects biometrics from all personnel accessing US bases, including soldiers, government employees, civilians, contractors, day workers, etc.	Ten Rolled Fingerprint, Photo, & Iris
Hand-held Interagency Identity Detection Equipment (HIIDE)	Tactical operations by OGA in Iraq, 10th Mtn Div in Afghanistan; also used in detention facilities	Flat Fingerprint, Photo, & Iris

DoD Biometric Strategy

FY 07				FY 08				FY 09				FY 10			
Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

Optimize What We Have

Support and sustain legacy systems

Increase capacity

SENSITIVE BUT UNCLASSIFIED

Biometrics Quick Look
Capabilities Based
Assessment

Joint Requirements
Oversight Council

28 September 2006

SENSITIVE BUT UNCLASSIFIED

Improve the Existing Architecture

Implement "Enterprise JUONS"

Down-Select "family of systems"

Field and Sustain "family of systems"

ic Priorities

Tactical/Operational Support Requirements	System Architecture and Data Base
#1 - Security Operations Plus-Up	#1 – System Architecture
#2 - Base Access	#2 – Data Access
	#3 – Tailorable Database
	#4 – Untethered Operations

UNCLASSIFIED//FOUO

Build What We Need

Full CBA

JCIDS

PR09 Wedge

POM 10 Build

System Spiral Program of record

Biometrics S&T Plan

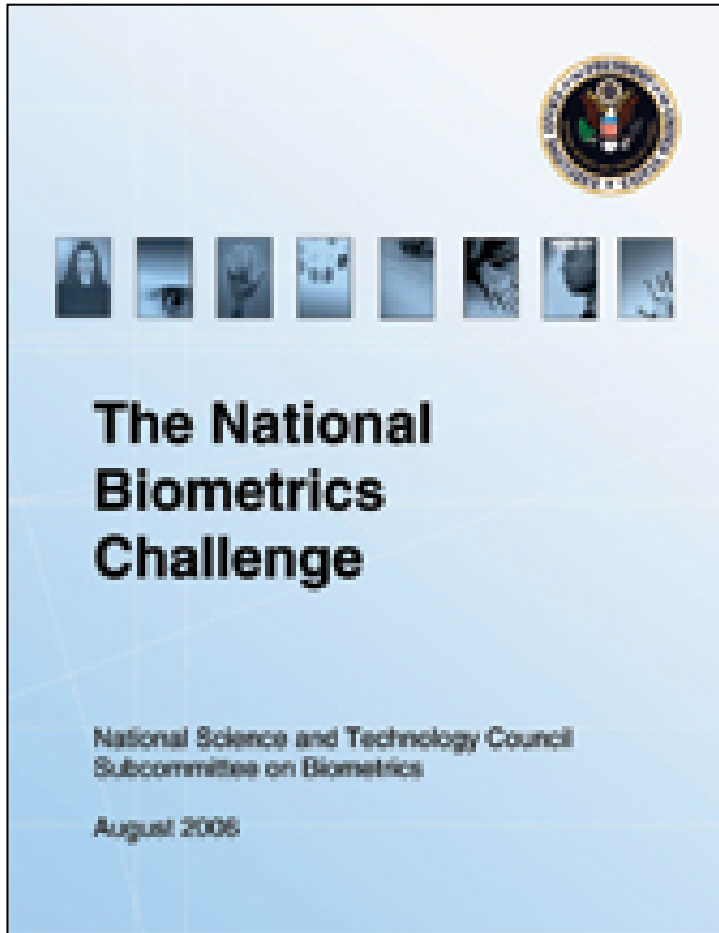**_Support immediate needs while building for the future_**

DOD Roles and Responsibilities

- **DDR&E is Principle Staff Assistant**

- **Army is Executive Agent**

- **EXCOM established as final arbitration forum and executive level collaborative forum**

- **Army established a joint governance structure subordinate to EXCOM**

  – **Full transparency of component biometrics programs**

- **Services retain Title 10 responsibilities**

Promote unity of effort to deliver desired outcomes

Technology Challenges

The National Biometrics Challenge

National Science and Technology Council
Subcommittee on Biometrics

August 2006

www.biometrics.gov

- **Improve Collection Devices**
  - **Biometrics Sensors**

- **Develop More Efficient and Effective large Scale operational Capabilities**
  - **Biometrics Systems**

- **Establish Standards for Plug and Play Performance**
  - **Systems interoperability**

- **Informed Debate on Why, How, and When Biometrics Should be Used**
  - **Biometrics Communications and Privacy**

Challenge

- **Biometrics is only a sub-set of Global Identity Management**

  - **Holistic program must support:**

    - **Combat applications & Business Functions & Intelligence source**

    - **Red Force & Blue Force & Neutrals**

    - **U.S. Persons & Non-U.S. persons**

    - **Verification & identification**

    - **Voluntary & involuntary subjects**

    - **Multi-service & Defense Agencies & Inter-agency & International**

    - **Biometrics & Credentials & Contextual data & Forensics**

    - **Privacy Data & Public Perceptions**

Goals

- 100% accuracy in identification and verification

- Interoperable biometrics systems within DoD & with Other Government Agencies

- Reduce workload and manpower associated with collection, storage, matching, analysis, & action

- Dramatically reduce latency in moving biometrics data and accelerating decisions
  - Hours … to minutes … to seconds (it was days & weeks)
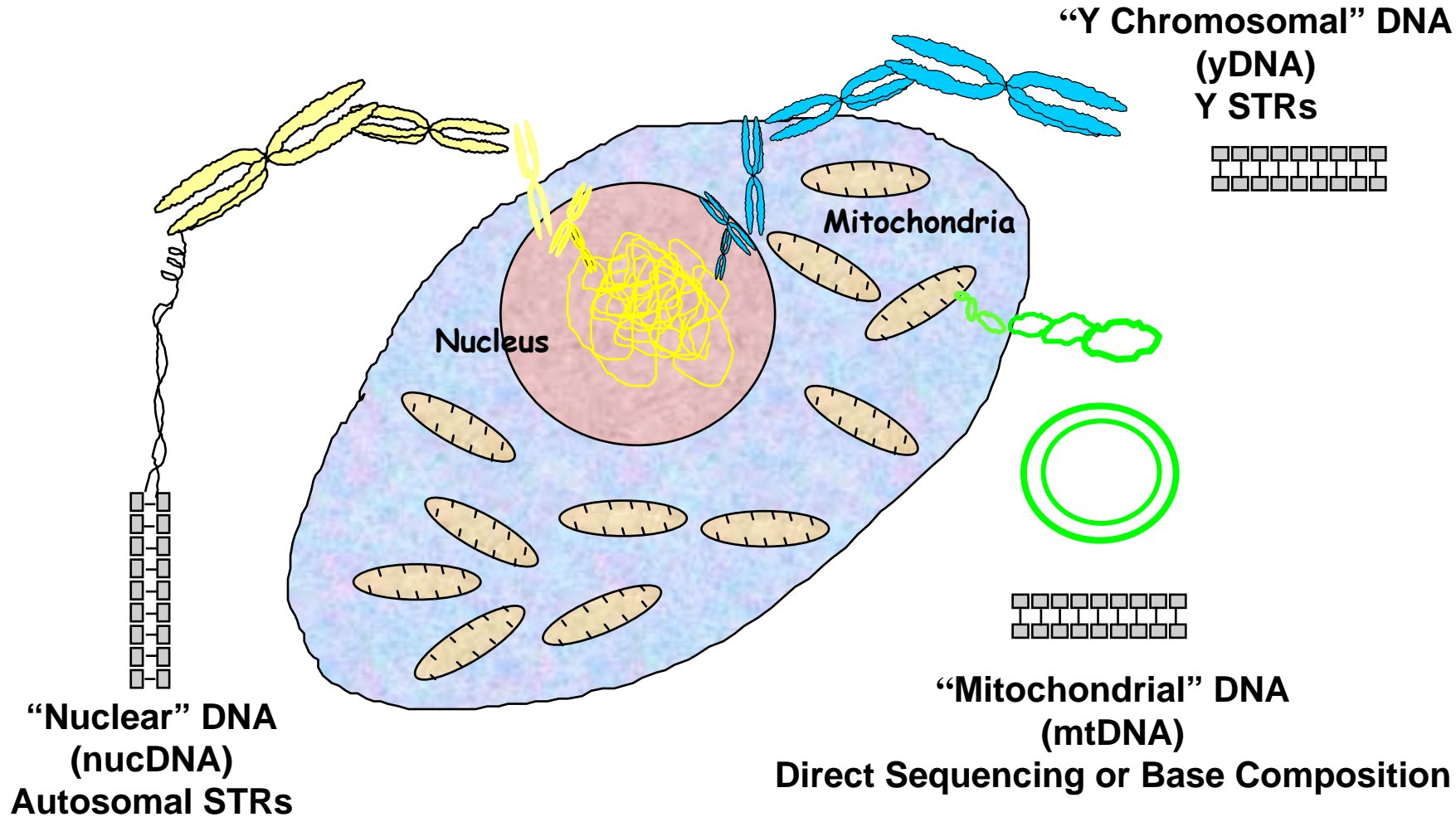
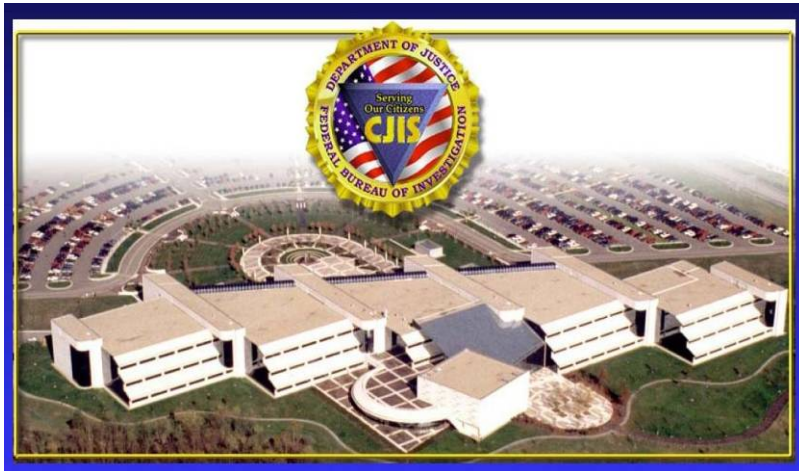*Synchronized, Integrated, Coordinated Program*

Discussion

Human Genome
as the subject of forensic analysis

"Y Chromosomal" DNA (yDNA) Y STRs

Mitochondria

Nucleus

"Nuclear" DNA (nucDNA) Autosomal STRs

"Mitochondrial" DNA (mtDNA) Direct Sequencing or Base Composition

9/7/2007

Integrated Automated Fingerprint Identification System (IAFIS)

The five key IAFIS services are:

1. Ten-print Based Fingerprint Identification Services

- Criminal submissions, responses within 2 hours

- Civil submissions, responses within 24 hours

- Supports DoD ABIS

2. Latent Fingerprint Services (at Quantico, VA)

3. Subject Search and Criminal History Services

4. Document and Imaging Services

5. Remote Ten-print and Latent Fingerprint Search Services

Owned by the FBI, IAFIS is the US National Fingerprint and Criminal History System

- Located at the Criminal Justice Information Services (CJIS) Division, Clarksburg, WV

- Maintains the world's largest biometrics database currently holding about 66 million records

- Has been in operation since July 1999

- Model for the DoD Automated Biometric Identification System (ABIS)

Automated Biometric Identification System (ABIS)

ABIS Background:

- Operational since July 2004
- Modeled after highly successful FBI system, Integrated Automated Fingerprint Identification System (IAFIS)
- Central repository for DoD biometric data
- Provides capability for searching, storing and matching biometrics data
- Building multi-modal searching/matching capability (NGEA)
- Located in Clarksburg, WV
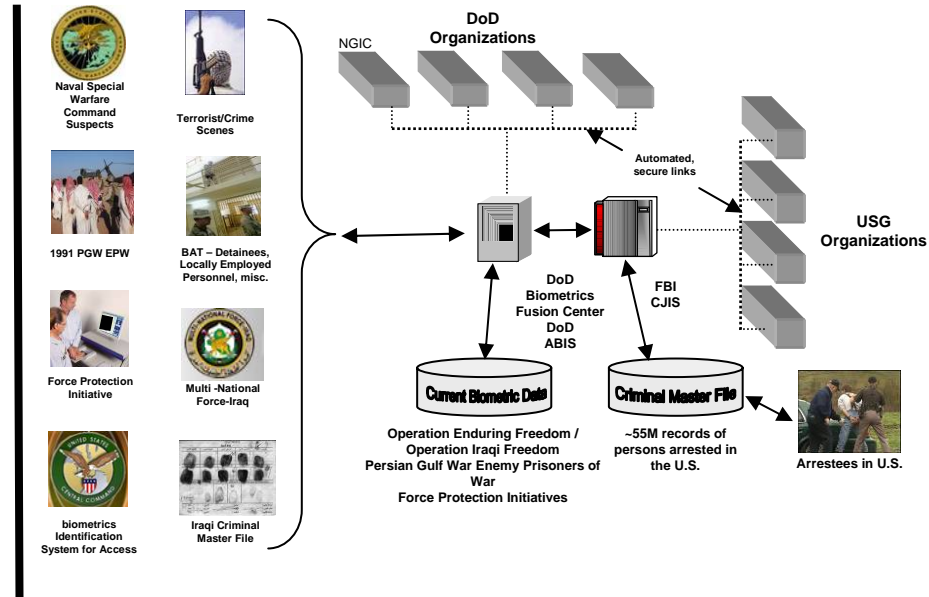
ABIS has made matches to:

- Known and suspected terrorists
- Bomb makers
- Passport forgers
- Individuals with US criminal convictions
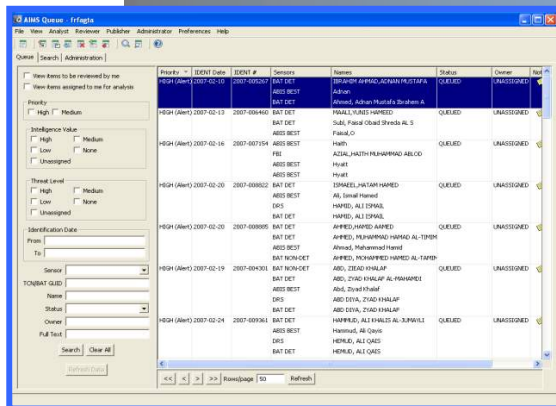- Former Iraqi criminals (Hussein regime)

ABIS Operations Tasks:

- Operate and maintain the ABIS repository
- Provide 24x7 biometrics matching services
- Share biometrics data with approved agencies
- Provide latent match capabilities
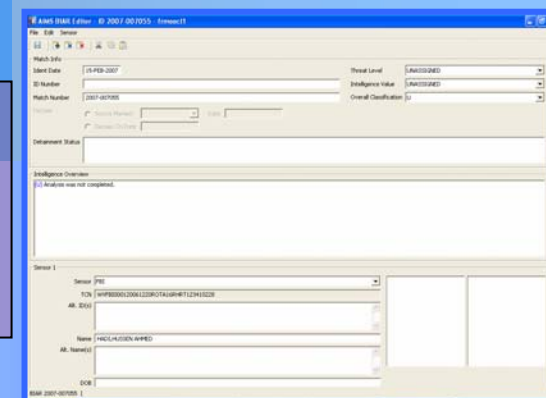
Automated Identity Management System (AIMS)

Analyst Workflow

- **Automated triage and Prioritization**
- **Focus on most significant Matches**
- **~ 4% of matches go in queue**

- **Consistent BIAR format**
- **Portion Markings**
- **Standardized classifications**
- **Posting to the WEB**
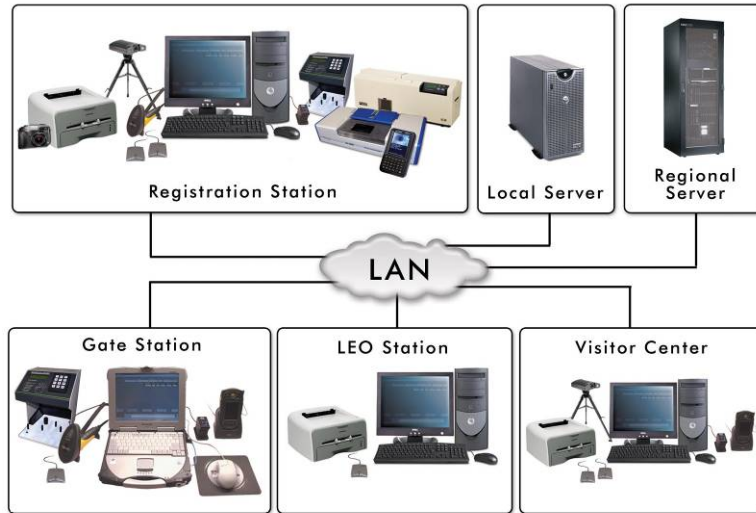
Production Tool

WEB Application

- **Searchable database that contains both BIARs and BMRs**
- **Soundex function**
- **Full Text search capability**

Defense Biometrics Identification System (DBIDS)

System:

Future Status:

- **Afghanistan – 10 Tier 1 sites long lead time items orders sent to GSA**
- **Navy Europe fielding to start July 2007 – 6 sites**
- **Navy CENTCOM (the island of Bahrain) fielding to begin August 2007**
- **Air Force CENTCOM – 6 sites to begin July 2007**
- **Japan – 2 sites in progress**
- **Guam – 3 sites planned**
- **Representatives from all services state they want their physical access systems in CONUS to be based on/interact with DBIDS**

Data Footprint:

- **Currently, DBIDS installed:**
  - **300 Gates**
  - **135 Installations (including USAREUR, SWA, USFK, and CONUS)**
  - **1.4M registrants**
- **DBIDS is the installation access control solution USFK and USAREUR-wide**
- **Attempted Accesses to DBIDS fielded Military Installations – Over 200 Million**
- **Accesses Denied – 1.5 Million**

Levels of Commitment:

- **Navy has signed MOU and has $ to field DBIDS Navy-wide**
- **CENTCOM has signed up for DBIDS at various sites in the AOR and will fund**
- **USAREUR and USFK are long-standing customers**
- **Representatives from all services state they want their physical access systems in CONUS to be based on/interact with DBIDS**
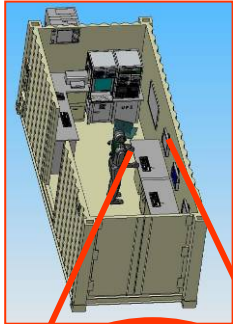- **DoD 5200.08R and 1000.25 both name DBIDS**

Prediction:
- **By end of calendar year 2007 DBIDS will be fielded at 330 Gates at 150 Installations, including USAREUR, SWA, USFK, USPACOM, and CONUS**
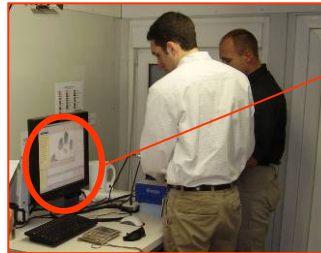
Biometric Identification System for Access - BISA

1. Enrollment Center and Kit

2. Iris-Scan and creation of digital image

3. Fingerprint Scan and creation of digital image

4. Digital biometric data loaded onto 'smart-card' BISA badge, with other contextual data.

5. Biometric data on badge verified ('one-to-one' match) by electronic readers at ECP.

Operational Concept

- Collect biometric data on all local- and third-country nationals (LN/TCN) accessing US bases in Iraq.

- Screens applicants against ABIS/IAFIS; If vetted then produces & issues access credential based on unique (person's) fingerprint & photo. Digitally verify biometric at each entry to assure identity.

- Electronic storage of biometric characteristics on 'smart-card' biometric template provides tamper-proof, forge-proof base-access credential, which also includes privilege (DFAC etc) eligibility and other commonly-required data. At verification (at ECP), electronically stored data is compared to individual data by all-electronic means; one-to-one match performed between digital image vs actual fingerprint of holder.

- Designed for turn-key deployment & operation in communications-austere and otherwise unfavorable (eg climate, dust, etc) environments.

National Detainee Reporting Center (NDRC)
Detainee Reporting System (DRS)

- **<u>Function</u>**: Provide total accountability and reporting of all biographic and biometric data for persons detained in association with the GWOT

- **<u>Scope</u>**:
  - DRS allows for real time data sharing with deployed systems
  - Independent satellite communication packages enable rapid transmittal of detainee information

- **<u>Capabilities</u>**:
  - DRS (v5.0) is web based
  - Issues Geneva Convention required Internment Serial Numbers
  - Collects and submits biometric fingerprints and photos with biographic information including medical and property files on all detainees
  - Contains an 'In Camp' management system and a 'Do Not Release' detainer option ensuring accuracy and preventing HVD releases

Biometrics Automated Toolset (BAT)

BAT Enrollment Station

Optional Equipment:

Digital Camera

Fingerprint Reader

500GB Hard Drive

Iris Scanner

Badge Printer

CF-73/74 Toughbook

Bar Code Scanner

- **Function:** BAT collects fingerprints, iris scans, facial photos and biographical information of persons of interest into a searchable data base.

- **Scope:** Over 2,000 systems deployed; 560,000+ biometrics enrollments

- **Mission Threads**: Tactical Operations, Force Protection, Detainee Operations, Population Control, Base Access, IED Forensics Operations, Special Operations, and Local Hire Screening / Intelligence

Handheld Interagency Identity Detection Equipment (HIIDE)

Fingerprint Sensor

Digital Face Camera

Iris Camera

5"

8"

Flash

IR Bar

Touch Screen Data Interface
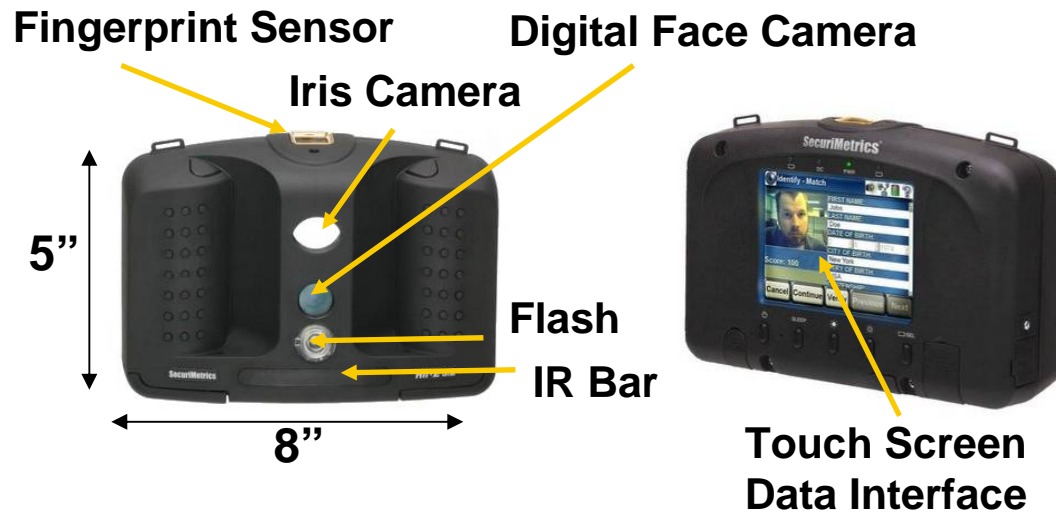
HIIDE Characteristics:

- **Lightweight (2lbs, 3 oz)**
- **Multimodal collection and matching device**
- **Interoperable with BAT for biometrics data exchange back to DoD biometrics Data Repository**

- **Function:** HIIDE collects and matches fingerprints, iris images, facial photos and biographical contextual data of Persons of Interest against an internal database.

- **Scope:** Major HIIDE fieldings since Oct 06: 900 OIF, 450 OEF, 250 USMC, 89 ISAF, and 45 SOF; planned total fielding of 6,664 devices

- **Mission Threads:** Tactical Operations, Force Protection, Detainee Operations, Access Control, Special Operations, and Intelligence Operations

Special Operations Identity Dominance (SOID) – Biometric Identification Kits

COMPONENTS

- Organic CF-18 Laptop
- Live Scan Management System (software)
- CrossMatch MV-5 Wand-style Print Reader
- Organic Team Comms Equipment

FUNDING INFORMATION

- Procurement (934 kits at $2K each): $1.9M
- O&M: $846K
- Total, FY 08-13: $2.7M

BOIP

75th Ranger Rgt: 80 (RGT = 14, BN = 21, CO = 18, PLT = 27)

USASFC: 651 (GRP = 7, BN = 56, ODB = 84 ODA = 504)

USACAPOC: 84 (BN = 4, CAT-A = 80)

USAJFKSWCS: 119 (1 system / student)

BACKGROUND

- ARSOF have unfunded requirement to capture, store, manipulate, transmit, & query against REDFOR and GRAYFOR biometric signatures in support of national strategic objectives and the GWOT.

- Identification kits are used for hold/release info in a tactical environment

- # 14 on USASOC Commander's Priority List

Special Operations Identity Dominance (SOID) – Biometric Enrollment Kits

COMPONENTS

- **Organic CF-18 Laptop**
- **Live Scan Management System (software)**
- **CrossMatch ID442 Scanner (10-print)**
- **Canon G-6 Digital Camera (f/ facial recognition)**
- **Iris Imager**
- **Organic Comms Equipment**

FUNDING INFORMATION

- **Procurement (714 kits at $10K each): $7.2M**
- **O&M: $3.2M**
- **Total, FY 08-13: $10.4M**

Fingerprint Scanner (and Cable)

Firewire Card

Power & Communications Cables

75th Ranger Rgt: 16 (RGT = 7, CO = 9)

USASFC: **651 (GRP = 7, BN = 56, ODB = 84, ODA = 504)**

USACAPOC: **20 (BN = 4, CO = 16)**

**USAJFKSWCS:**   **27 (5 students / system)**

BACKGROUND

- **ARSOF have an unfunded requirement to capture, store, manipulate, transmit, & query against REDFOR and GRAYFOR biometric signatures in support of national strategic objectives and the GWOT.**

- **Enrollment kits are for full enrollments in less austere environments**

- **# 15 on USASOC Commander's Priority List**

Navy MIO Collection Systems
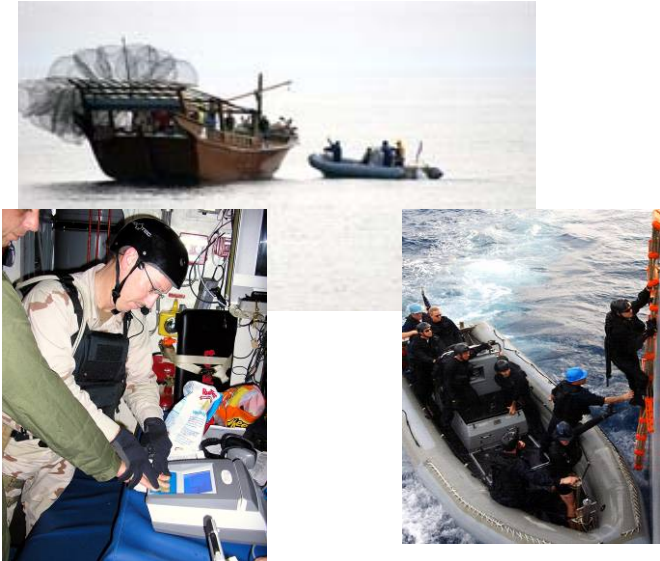
Operational Concept

The fundamental purpose of the Identity Dominance System (IDS) is to provide the capability to positively enroll, identify, and verify the identity of personnel. This capability is expected to play a key role in the Global War on Terrorism (GWOT) and the full range of military operations. The Tactical Biometrics Collection and Matching System (TBCMS) will be fielded using the IDS spiral one requirements as a quick reaction response to a CENTCOM JUONS. The BFC provides Subject Matter Experts to the Navy in support of IDS

Technical Approach & Milestones

- Approved at eR3B – Nov06
- Staffed in Joint Staffing Process; modified CDD due to Joint Staff – 2 Mar 07
- Significant modifications made
- Back to Phase 1 staffing 18Jun07
- BAWG – Aug07
- FCB – Sep07
- MS B – Jan 08
- MS C – Oct 08
- IOC – Dec 08

Challenges

- Responsibility for adjudication of matches currently resides with the commanding officer of the vessel dispatching the VBSS team (ONI will receive match response)
- System for passing data between boarded vessel and host vessel in development
- Funding for TBCMS follow on systems/IDS not yet secured

Expanded Maritime Interception Operations (EMIO)

Equipment Description:
- Pelican 1600 Case
- CMT ID442R
  - 8.8Lbs
  - Sealed Aluminum
  - FBI Certified
  - 500DPI Optical
  - Slaps and Rolls
- BB2590/5590 Battery
- Panasonic CF-18F
- Panasonic IRIS
- Olympus D595 5.1 MPX Digital Camera
- Capable of 10 prints – rolls/slaps
- <18 Watts power requirement
- 12 VDC Battery with converter
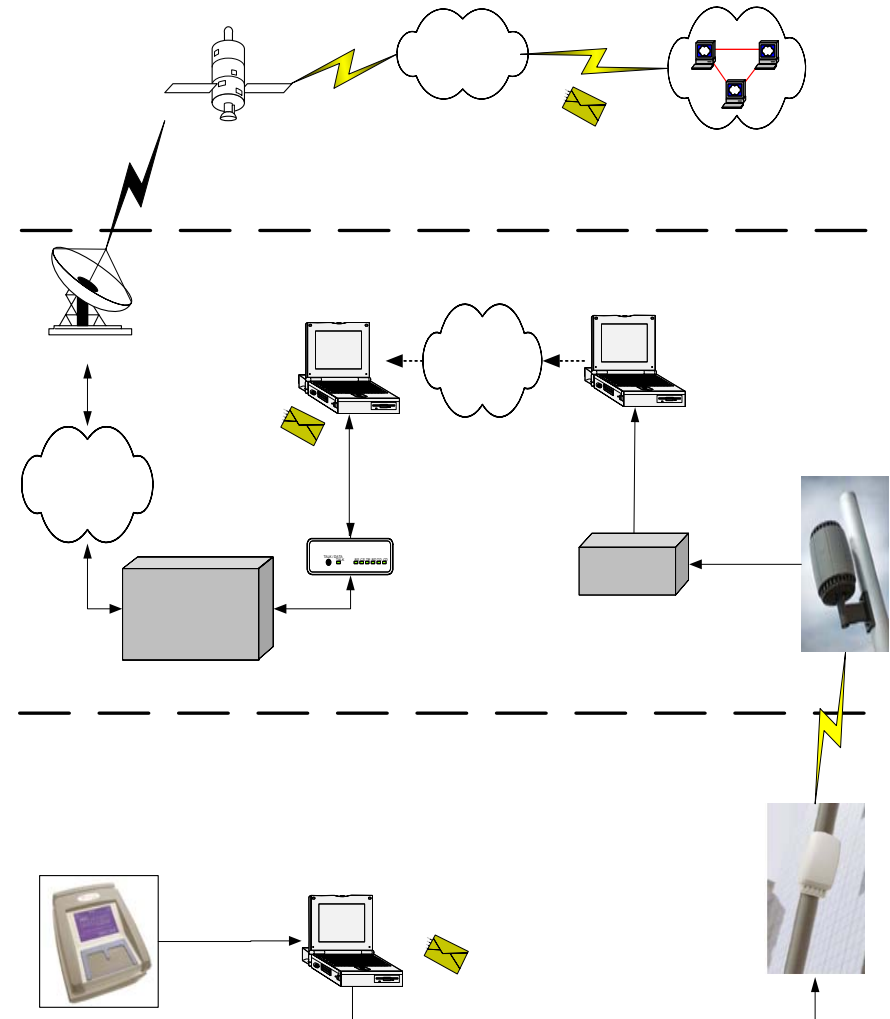
Biometrics S&T

- **Develop a DoD Science and Technology (S&T) Road-map**
  - **Synchronized with interagency**
  - **Transition goals to acquisition**

- **Accelerate longer-range advanced technologies**

- **Potential Opportunities:**
  - **Iris-at-a-Distance**
  - **Facial Recognition**
  - **Non-Obtrusive Biometrics**
  - **Rapid Fingerprint Capture**
  - **Enhanced Latent Fingerprint Detection**
  - **Natural Forensics for Backtracking Terrorists**
  - **Biometrics Operational Exchange**
  - **Multimodal Biometrics Fusion**
  - **Standards Development & Prototype Deployments**
  - **Improved Data Storage and Exchange**
    - **Wireless systems, data architectures, data standards, system form factors to permit expeditionary operations**