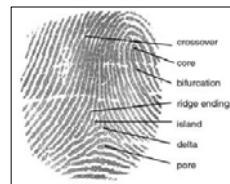# DoD Biometrics

Biometrics Consortium Conference

13 Sep 2007

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

Agenda

- **Background** (Mr Tom Dee, OSD AT&L, DDR&E)

- **Biometrics in Support of GWOT** (Dr Myra Gray, Director, USA BTF)

- **NORTHCOM** (Mr Frank Lugo)

- **Navy** (Ms Anh Duong, OPNAV N3 Science Advisor)

- **USMC** (LtCol John Manson, HQ USMC PP&O)

- **Q&A** (Dee, Gravell, Gray, Lugo, Duong, Manson)

Outline

- **Background**
  - **One Problem**
  - **Traditional Solutions**
  - **Technology**

- **DoD Biometrics**
  - **Mission**
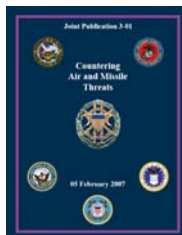 - **Strategy**
  - **Organization**

- **Challenges**

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

"People"

"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."
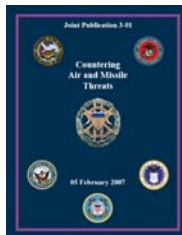
Joint Pub 3-01, 5 Feb 2007

Combat Identification

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

Shapes?

Markings?

Signatures?

Signals?

Platforms

People

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

Enemy?

Neutral?

Friend?

Classification

Friend / Enemy / Neutral ?

- **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

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

Detection technology

Deterrence

Alert Zone

Exclusion Zone

Situational Awareness Zone 10-15 km
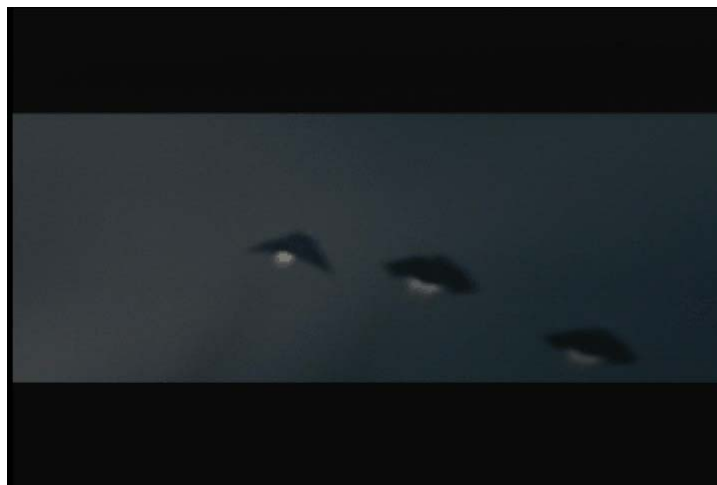
The Material Solution…

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

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

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**
    - **IA, Credentials, etc…**
  - **Privilege management**
    - **Health care, benefits, finance, time and attendance, etc.**

- **Military operations**
  - **"Combat Identification"**

    - **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

Traditional Functions

- **A "verification" task to support…**
  - **Physical and logical Access**
  - **Information assurance**
  - **Privilege Management**

DoD 5200.08-R

PHYSICAL SECURITY PROGRAM

April 9, 2007

UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
(USD(I))

Department of Defense
DIRECTIVE

NUMBER 1000.25
July 19, 2004
Certified Current as of April 23, 2007
USD(P&R)

SUBJECT: DoD Personnel Identity Protection (PIP) Program

**Base Access
Aviano Air Base (AB), Italy**

**Logical Access Controls with
Common Access Card (CAC)**

The "Identification" Task

Supporting Requirements

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

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

Biometrics Quick Look
Capabilities Based
Assessment

Joint Requirements
Oversight Council

28 September 2006

Improve the Existing Architecture

Implement "Enterprise JUONS"

Down-Select "family of systems"

Field and Sustain "family of systems"

Priorities

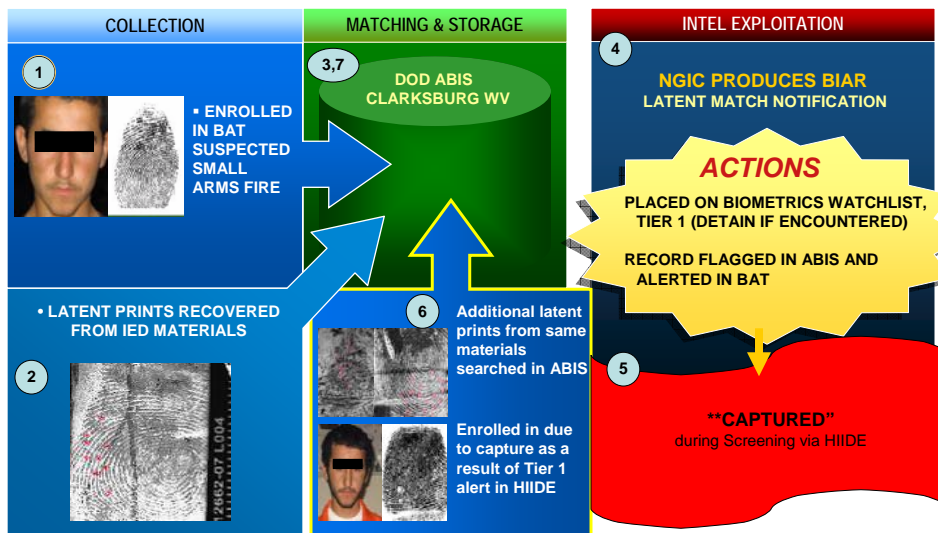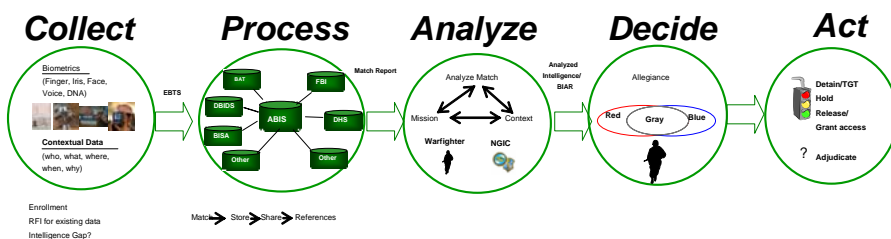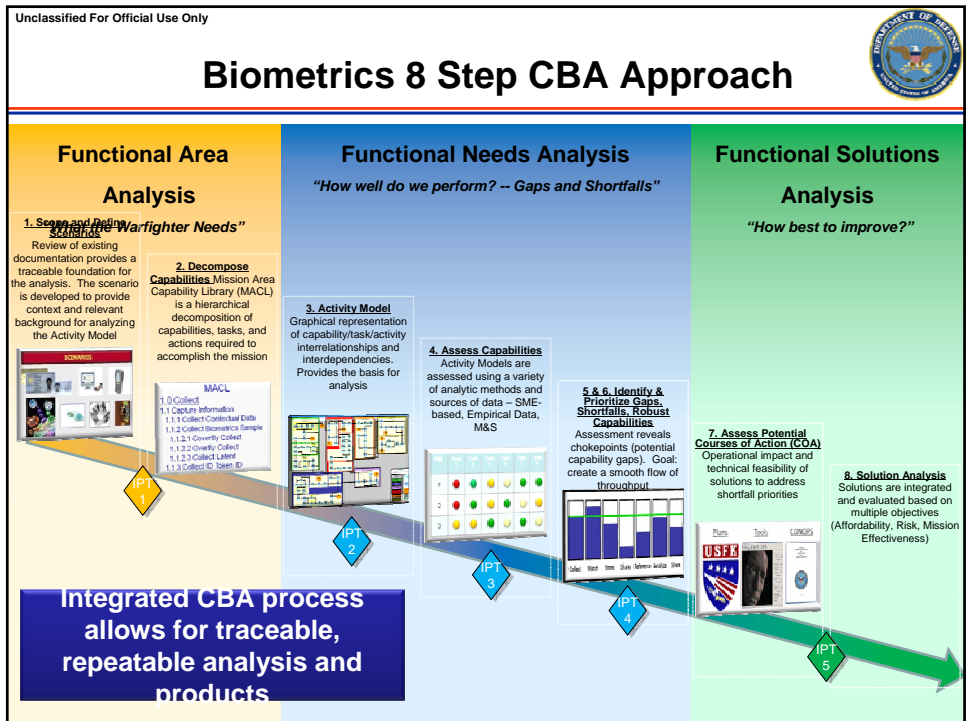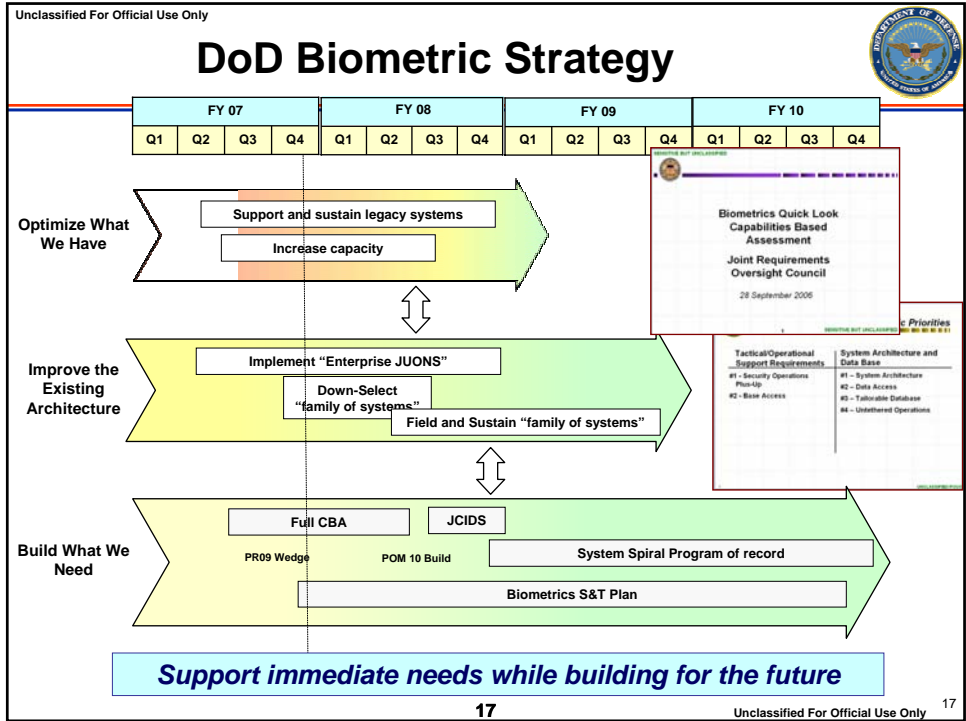| Tactical/Operational Support Requirements	System Architecture and Data Base
#1 - Security Operations Plus-Up	#1 - System Architecture
#2 - Base Access	#2 - Data Access
	#3 - Tailorable Database
	#4 - Untethered Operations

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

17

Biometrics 8 Step CBA Approach

Functional Area Analysis

Functional Needs Analysis
"How well do we perform? -- Gaps and Shortfalls"

Functional Solutions Analysis
"How best to improve?"

1. Scope and Define Scenarios *"Determine Warfighter Needs"*
Review of existing documentation provides a traceable foundation for the analysis. The scenario is developed to provide context and relevant background for analyzing the Activity Model

2. Decompose Capabilities Mission Area Capability Library (MACL) is a hierarchical decomposition of capabilities, tasks, and actions required to accomplish the mission

3. Activity Model Graphical representation of capability/task/activity interrelationships and interdependencies. Provides the basis for analysis

4. Assess Capabilities Activity Models are assessed using a variety of analytic methods and sources of data – SME-based, Empirical Data, M&S

5 & 6. Identify & Prioritize Gaps, Shortfalls, Robust Capabilities Assessment reveals chokepoints (potential capability gaps). Goal: create a smooth flow of throughput

7. Assess Potential Courses of Action (COA) Operational impact and technical feasibility of solutions to address shortfall priorities

8. Solution Analysis Solutions are integrated and evaluated based on multiple objectives (Affordability, Risk, Mission Effectiveness)

SCENARIOS:

MACL
1.0 Collect
1.1 Capture Information
1.1.1 Collect Contextual Data
1.1.2 Collect Biometrics Sample
1.1.2.1 Covertly Collect
1.1.2.2 Overtly Collect
1.1.2.3 Collect Latent
1.1.3 Collect ID Token ID

IPT 1

IPT 2

IPT 3

IPT 4

IPT 5

Integrated CBA process allows for traceable, repeatable analysis and products

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
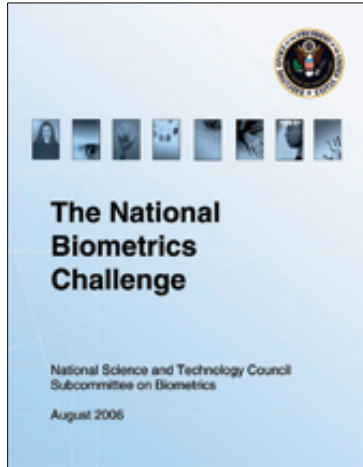

Challenge

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

  - **Holistic program must support:**

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

    - **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**

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**

Goals

- **100% accuracy in identification and verification**

- **Interoperable biometrics systems within DoD & with Other Government Agencies**

- **Improve security posture while gaining efficiencies**

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

Synchronized, Integrated, Coordinated Program

Discussion

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**