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

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 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

- Tactical decisions require:
  - Detection
  - Classification

- 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
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

Alert Zone
Exclusion Zone
Situational Awareness Zone/10-15 km

Deterrence
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 one-to-one matching process

Identification – a one-to-many 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

- **Confidence level of ID?**
- **Consequences of a wrong ID?**
- **Operational situation?**
- **ROE?**

Traditional Functions

- A “verification” task to support…
  - Physical and logical Access
  - Information assurance
  - Privilege Management

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

- **Logical Access Controls with Common Access Card (CAC)**
The "Identification" Task

1. Collection
   - Enrolled in BAT suspected small arms fire
   - Latent prints recovered from IED materials

2. Matching & Storage
   - ROD ABIS
   - CLARKSBURG WV
   - Additional latent prints from same materials searched in ABIS

3. Intel Exploitation
   - NGIC produces BIAR latent match notification
   - Placed on biometrics watchlist, Tier 1 (detain if encountered)
   - Record flagged in ABIS and alerted in BAT

4. Actions
   - "Captured" during screening via HIIDE

Supporting Requirements

- Sensors to collect
- Databases to store
  - Data to match
    - Biometric forensics
- Applications to process
- Communications to share
- Analysis tools for decision support
Optimize What We Have

Improve the Existing Architecture

Build What We Need

Support immediate needs while building for the future

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

Support and sustain legacy systems

Increase capacity

Improve

Implement "Enterprise JUONS"

Down-Select "family of systems"

Field and Sustain "family of systems"

Build

Full CBA

JCIDS

PRB Workbook

POM 10 Build

System Spiral Program of record

Biometrics S&T Plan

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?”

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

- 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