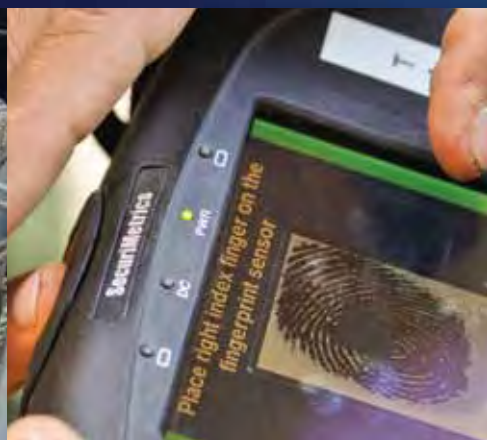# ANNUAL REPORT FY10
## IDENTIFY/ENABLE/PROTECT

**BIMA** BIOMETRICS IDENTITY MANAGEMENT AGENCY

U.S. Soldiers with Alpha Company, 1st Battalion, 17th Infantry Regiment collect biometrics and conduct searches during Operation Moshtarak in Badula Qulp, Helmand province, Afghanistan, Feb. 21, 2010.  (U.S. Air Force photo by TSgt Efren Lopez)

# TABLE OF CONTENTS

U.S. Soldiers biometrically enroll Afghan men at the Torkham Gate border crossing site.
(BIMA photo by LTC William Buhrow, U.S. Army)

## DIRECTOR'S MESSAGE

Fiscal Year 2010 was a watershed year for the Biometrics Identity Management Agency (BIMA).  As we continued to grow and mature as an organization, we also took a significant step toward becoming a permanent Department of Defense (DoD) component. On October 26, 2009, the Vice Chief of Staff of the Army directed the redesignation of the Biometrics Task Force (BTF) as the BIMA and recommended the establishment of the BIMA as a Field Operating Agency.

This critical move ensures that the BIMA will become a permanent organization rather than remain a temporary task force and provides the structure and support necessary for biometrics to endure as an enabling capability for the DoD. On March 23, 2010, the Secretary of the Army officially redesignated the BTF as the BIMA.

The process to finalize the BIMA status as a permanent Field Operating Agency is still underway.  This transformation reflects both the successes biometrics have had in supporting the warfighter and protecting our country and allies from terrorism and the vision of what biometrics can bring to the DoD in the future.

This past year also saw the BIMA move ahead in several key areas. The DoD Automated Biometric Identification System continued to receive, retrieve, match and store thousands of records sent from around the globe.

We sponsored the first DoD Biometrics Collaboration Forum, held in January 2010. The forum was designed to bring together the biometrics community for a "roll up your sleeves" approach to urgent issues concerning the use of biometrics within the DoD and other federal agencies. Nearly 300 attendees discussed topics focused on enemy and friendly identification operations and architecture.

The BIMA facilitated and participated in the establishment of additional interagency and international agreements and Memoranda of Understanding, and supported expanded collaboration efforts. In doing so, the BIMA made significant 9/11-related biometrics matches. The interoperability process with the Department of Homeland Security also gained momentum this past year. The BIMA played a key role in introducing and incorporating biometrics capabilities into the North Atlantic Treaty Organization.  By collaborating with partners such as the United Kingdom's New Scotland Yard, there have been successful matches to DoD biometrics records of former Guantanamo Bay, Cuba, detainees.

Emphasis on friendly-force biometrics continues to grow.  We are making significant progress toward integrating biometrics into DoD business functions to increase efficiency, effectiveness and accuracy by validating access permissions.

Lastly, on July 13, 2010, we celebrated 10 years of DoD biometrics.  In this short time, DoD biometrics has evolved from a focus on information assurance to serving as a cornerstone enabler of identity management. Biometrics capabilities deny anonymity to our adversaries and verify individuals' identities for purposes such as controlled access to DoD facilities.  We appreciate your interest in and support of DoD biometrics as we look forward to the next 10 years.

Sincerely,
Dr. Myra S. Gray

# IDENTIFY/ENABLE/PROTECT

"Identify, Enable, Protect" articulates the BIMA core capability (**identify**), its utilization in security and business operations (**enable**) and its national security purpose (**protect**).

Biometrics is a key capability that can identify the enemy, denying him the anonymity he needs to hide and strike at will. The ability to identify and verify individuals is also critical to ensure secure and expeditious business functions. As these biometrics capabilities are applied through various tactics, techniques and processes, they enable a wide range of possible missions, from military operations to business functions, that protect national interests. In business, biometrics capabilities can protect as well as expedite business processes.
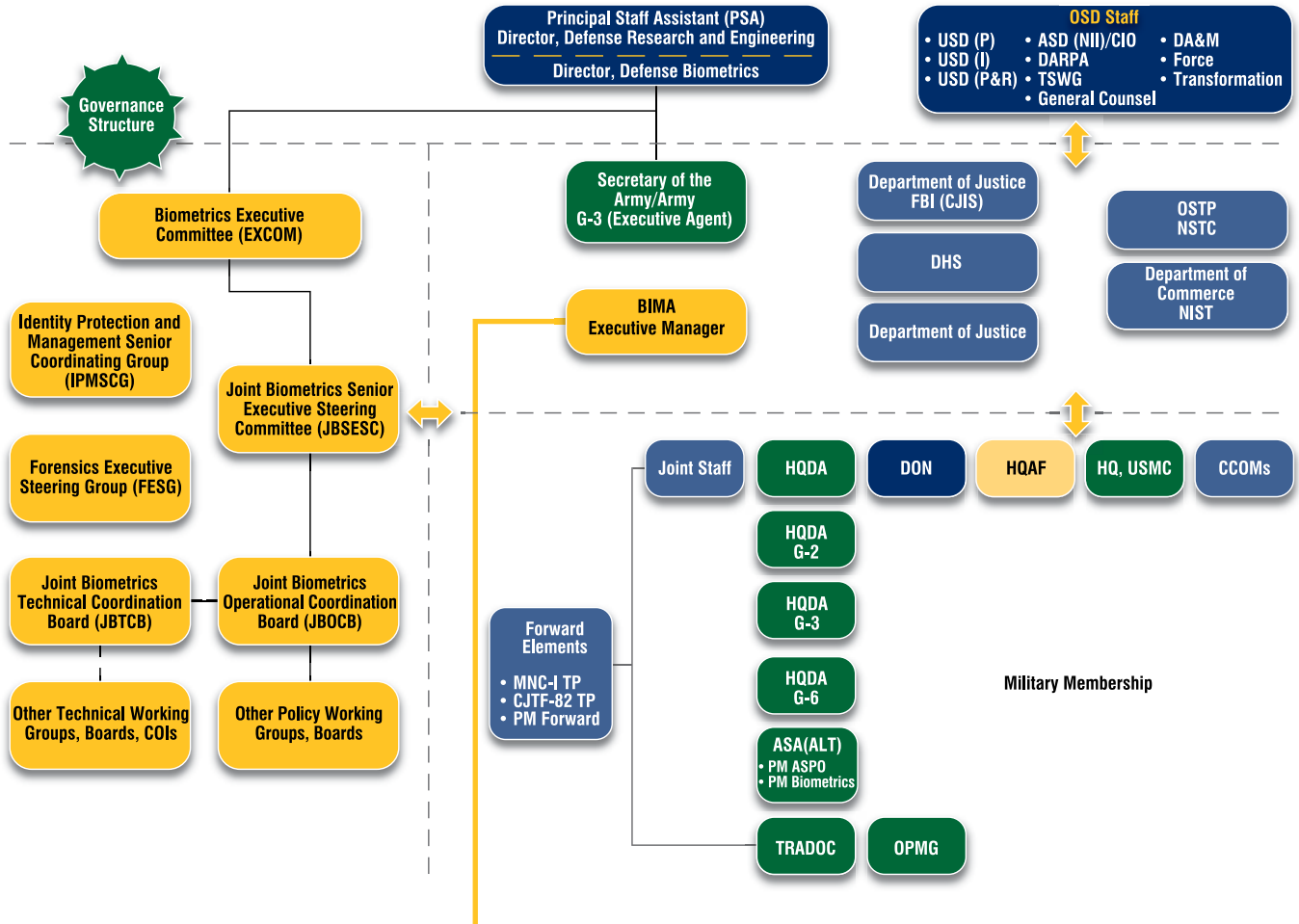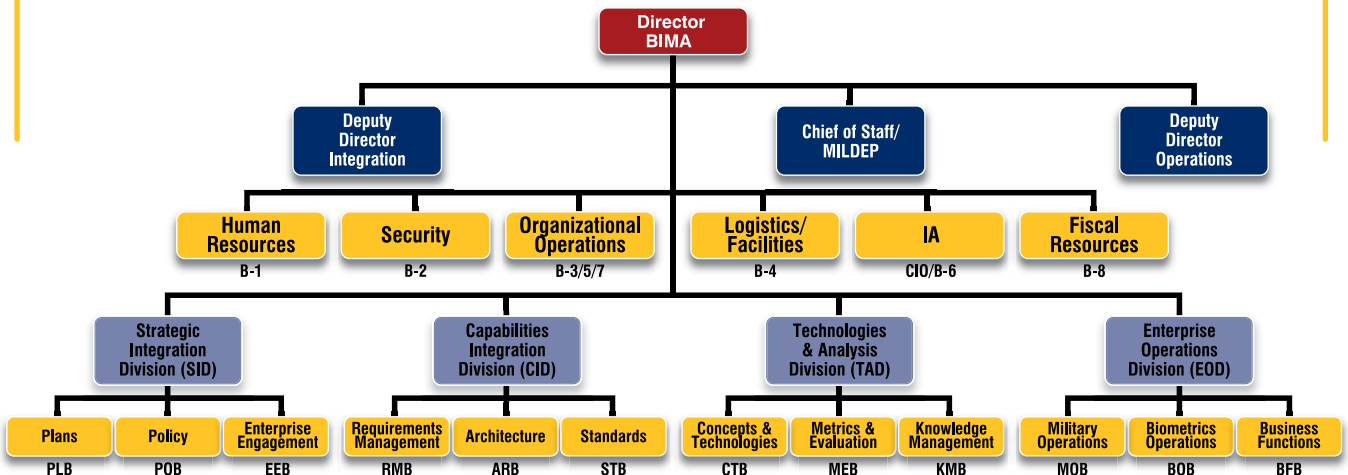
# ABOUT THE BIMA

## BIMA MISSION
The BIMA mission is to lead DoD activities to program, integrate and synchronize biometrics technologies and capabilities and to operate and maintain the DoD authoritative biometrics database in support of the National Security Strategy.

# ORGANIZATION STRUCTURE

## DoD BIOMETRICS: STRUCTURE

**Principal Staff Assistant (PSA)**
**Director, Defense Research and Engineering**

**Director, Defense Biometrics**

**OSD Staff**
- USD (P)   • ASD (NII)/CIO   • DA&M
- USD (I)   • DARPA           • Force
- USD (P&R)  • TSWG           • Transformation
- General Counsel

**Governance Structure**

**Biometrics Executive Committee (EXCOM)**

**Secretary of the Army/Army G-3 (Executive Agent)**

**Department of Justice FBI (CJIS)**

**OSTP NSTC**

**Identity Protection and Management Senior Coordinating Group (IPMSCG)**

**Joint Biometrics Senior Executive Steering Committee (JBSESC)**

**BIMA Executive Manager**

**DHS**

**Department of Commerce NIST**

**Forensics Executive Steering Group (FESG)**

**Department of Justice**

**Joint Biometrics Technical Coordination Board (JBTCB)**

**Joint Biometrics Operational Coordination Board (JBOCB)**

**Joint Staff** | **HQDA** | **DON** | **HQAF** | **HQ, USMC** | **CCOMs**

**Other Technical Working Groups, Boards, COIs**

**Other Policy Working Groups, Boards**

**HQDA G-2**

**Forward Elements**
- MNC-I TP
- CJTF-82 TP
- PM Forward

**HQDA G-3**

**HQDA G-6**

**Military Membership**

**ASA(ALT)**
- PM ASPO
- PM Biometrics

**TRADOC** | **OPMG**

## BIMA ORGANIZATION CHART

**Director BIMA**

**Deputy Director Integration**

**Chief of Staff/ MILDEP**

**Deputy Director Operations**

| **Human Resources** | **Security** | **Organizational Operations** | **Logistics/ Facilities** | **IA** | **Fiscal Resources** |
|---|---|---|---|---|---|
| B-1 | B-2 | B-3/5/7 | B-4 | CIO/B-6 | B-8 |

**Strategic Integration Division (SID)**

**Capabilities Integration Division (CID)**

**Technologies & Analysis Division (TAD)**

**Enterprise Operations Division (EOD)**

| **Plans** | **Policy** | **Enterprise Engagement** | **Requirements Management** | **Architecture** | **Standards** | **Concepts & Technologies** | **Metrics & Evaluation** | **Knowledge Management** | **Military Operations** | **Biometrics Operations** | **Business Functions** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PLB | POB | EEB | RMB | ARB | STB | CTB | MEB | KMB | MOB | BOB | BFB |

A U.S. Army Soldier uses the Handheld Interagency Identity Detection Equipment (HIIDE) system to create a biometrics profile of a local villager. The data will be used to ensure security by preventing known threats from disrupting the village medical operation. (Source: Public Intelligence)

## STRATEGIC FOCUS

The DoD Biometrics Enterprise is an entity comprised of the Department's joint, Service and agency organizations working together to integrate biometrics into the identity transactions needed to support military operations and departmental business functions. The DoD Biometrics Enterprise mission is to provide enduring biometrics capabilities to the DoD and its mission partners and enable identification of individuals in support of national security interests. It envisions a flexible, global biometrics enterprise that protects rights and enables services for friends and partners and denies anonymity to adversaries. The Biometrics Enterprise Strategic Plan (BESP) sets the strategic direction for the Enterprise and has established four goals, derived from DoD goals:
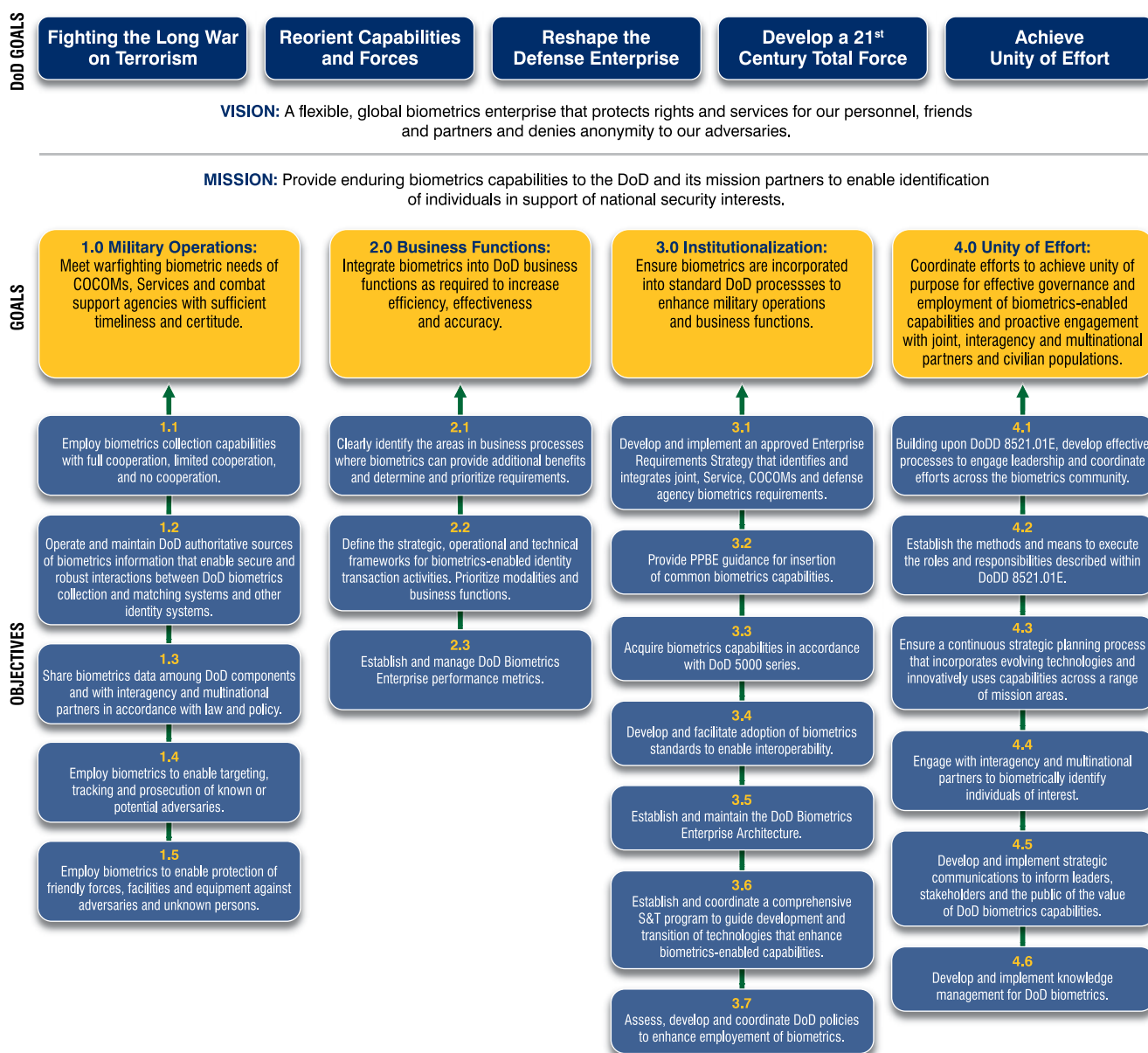
- **Military Operations** — Meet warfighting biometrics needs of Combatant Commands (COCOMs), Services and Combat Support Agencies with sufficient timeliness and certitude.
- **Business Functions** — Integrate biometrics into DoD business functions as required to increase efficiency, effectiveness and accuracy.
- **Institutionalization** — Ensure biometrics are incorporated into standard DoD processes in order to enhance military operations and business functions.

- **Unity of Effort** — Coordinate efforts to achieve unity of purpose for the effective governance and employment of biometrics-enabled capabilities and proactive engagement with joint, interagency and multinational partners and civilian populations.

These strategic goals have 21 supporting objectives. The BESP Goals and Objectives articulate the DoD Biometrics Enterprise — and therefore BIMA — priorities. BIMA fiscal year 2010 (FY10) accomplishments describe progress towards the BESP.

## DoD BIOMETRICS ENTERPRISE STRATEGY MAP

**DoD GOALS**

| Fighting the Long War on Terrorism | Reorient Capabilities and Forces | Reshape the Defense Enterprise | Develop a 21st Century Total Force | Achieve Unity of Effort |
|---|---|---|---|---|

**VISION:** A flexible, global biometrics enterprise that protects rights and services for our personnel, friends and partners and denies anonymity to our adversaries.

**MISSION:** Provide enduring biometrics capabilities to the DoD and its mission partners to enable identification of individuals in support of national security interests.

**GOALS**

| 1.0 Military Operations: Meet warfighting biometric needs of COCOMs, Services and combat support agencies with sufficient timeliness and certitude. | 2.0 Business Functions: Integrate biometrics into DoD business functions as required to increase efficiency, effectiveness and accuracy. | 3.0 Institutionalization: Ensure biometrics are incorporated into standard DoD processses to enhance military operations and business functions. | 4.0 Unity of Effort: Coordinate efforts to achieve unity of purpose for effective governance and employment of biometrics-enabled capabilities and proactive engagement with joint, interagency and multinational partners and civilian populations. |
|---|---|---|---|

**OBJECTIVES**

**1.1**
Employ biometrics collection capabilities with full cooperation, limited cooperation, and no cooperation.

**1.2**
Operate and maintain DoD authoritative sources of biometrics information that enable secure and robust interactions between DoD biometrics collection and matching systems and other identity systems.

**1.3**
Share biometrics data amoung DoD components and with interagency and multinational partners in accordance with law and policy.

**1.4**
Employ biometrics to enable targeting, tracking and prosecution of known or potential adversaries.

**1.5**
Employ biometrics to enable protection of friendly forces, facilities and equipment against adversaries and unknown persons.

**2.1**
Clearly identify the areas in business processes where biometrics can provide additional benefits and determine and prioritize requirements.

**2.2**
Define the strategic, operational and technical frameworks for biometrics-enabled identity transaction activities. Prioritize modalities and business functions.

**2.3**
Establish and manage DoD Biometrics Enterprise performance metrics.

**3.1**
Develop and implement an approved Enterprise Requirements Strategy that identifies and integrates joint, Service, COCOMs and defense agency biometrics requirements.

**3.2**
Provide PPBE guidance for insertion of common biometrics capabilities.

**3.3**
Acquire biometrics capabilities in accordance with DoD 5000 series.

**3.4**
Develop and facilitate adoption of biometrics standards to enable interoperability.

**3.5**
Establish and maintain the DoD Biometrics Enterprise Architecture.

**3.6**
Establish and coordinate a comprehensive S&T program to guide development and transition of technologies that enhance biometrics-enabled capabilities.

**3.7**
Assess, develop and coordinate DoD policies to enhance employement of biometrics.

**4.1**
Building upon DoDD 8521.01E, develop effective processes to engage leadership and coordinate efforts across the biometrics community.

**4.2**
Establish the methods and means to execute the roles and responsibilities described within DoDD 8521.01E.

**4.3**
Ensure a continuous strategic planning process that incorporates evolving technologies and innovatively uses capabilities across a range of mission areas.

**4.4**
Engage with interagency and multinational partners to biometrically identify individuals of interest.

**4.5**
Develop and implement strategic communications to inform leaders, stakeholders and the public of the value of DoD biometrics capabilities.

**4.6**
Develop and implement knowledge management for DoD biometrics.

Approved as of August 27, 2008; updates in progress.

## GOVERNING THE ENTERPRISE

Due to the increased biometrics activity across the DoD, the Department established a joint biometrics governance structure to coordinate biometrics strategies, policy, concepts, standards and requirements across the Biometrics Enterprise.
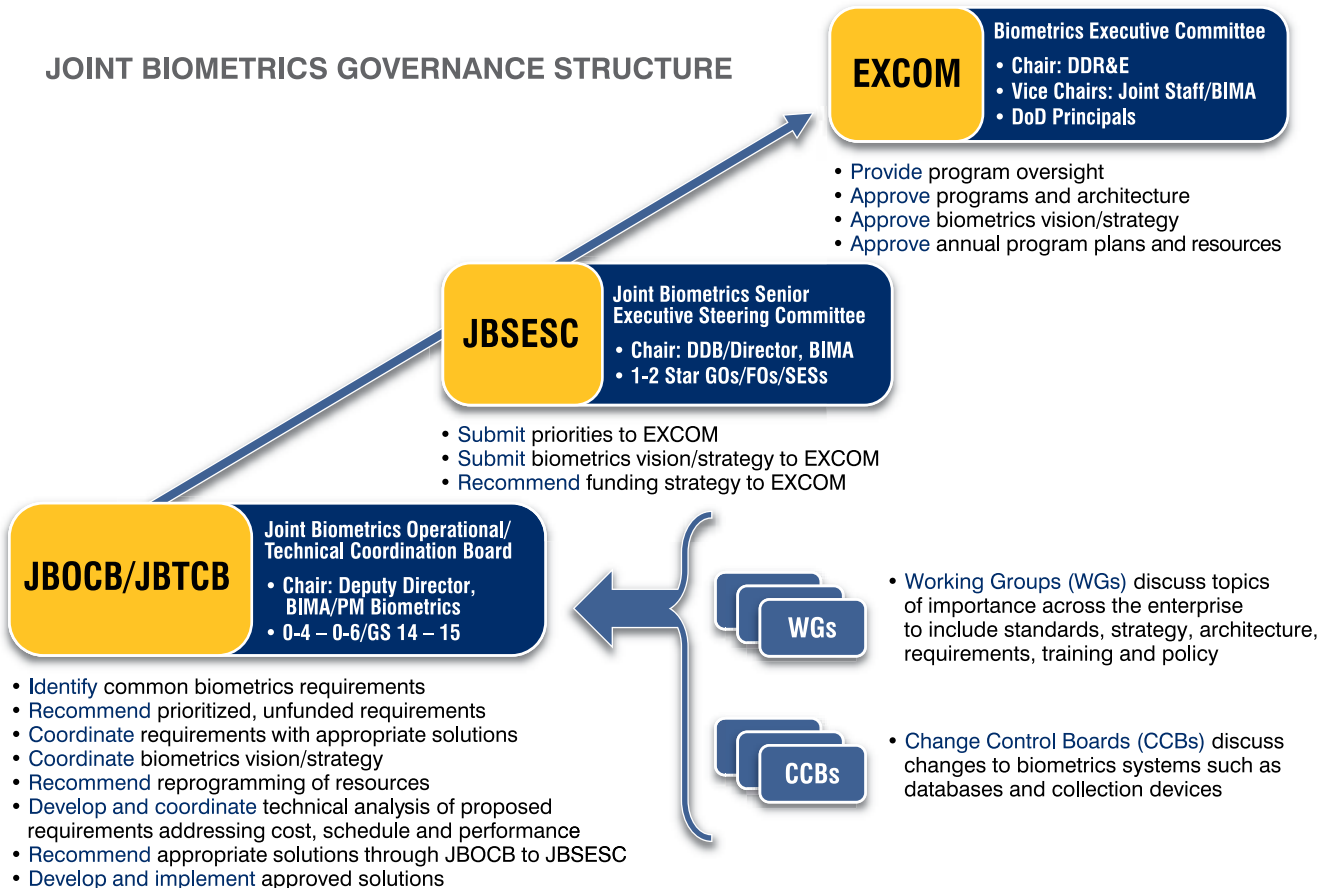
The Biometrics Executive Committee (EXCOM) serves as the focal point and voice to ensure coordination of biometrics requirements, acquisition programs and resources in support of the most operationally relevant and sustainable biometrics capabilities across the DoD.

The Joint Biometrics Senior Executive Steering Committee executes task assignments from the EXCOM and submits biometrics requirements priorities, funding strategy in support of capabilities across the Biometrics Enterprise and the biometrics vision and strategy to the EXCOM.

The Joint Biometrics Operational Coordination Board (JBOCB) and Joint Biometrics Technical Coordination Board (JBTCB) operate in tandem to bridge the gap between operational and technical issues, requirements and initiatives. The JBOCB oversees working groups and the JBTCB oversees Change Control Boards (CCBs). The CCBs and working groups focus, research and frame specific topics in support of the biometrics governing bodies; identify and/or address potential change recommendations; and elevate findings and recommendations through the joint biometrics governance process.

## JOINT BIOMETRICS GOVERNANCE STRUCTURE



**EXCOM**
**Biometrics Executive Committee**
- Chair: DDR&E
- Vice Chairs: Joint Staff/BIMA
- DoD Principals

- Provide program oversight
- Approve programs and architecture
- Approve biometrics vision/strategy
- Approve annual program plans and resources

**JBSESC**
**Joint Biometrics Senior Executive Steering Committee**
- Chair: DDB/Director, BIMA
- 1-2 Star GOs/FOs/SESs

- Submit priorities to EXCOM
- Submit biometrics vision/strategy to EXCOM
- Recommend funding strategy to EXCOM

**JBOCB/JBTCB**
**Joint Biometrics Operational/ Technical Coordination Board**
- Chair: Deputy Director, BIMA/PM Biometrics
- 0-4 – 0-6/GS 14 – 15

- Identify common biometrics requirements
- Recommend prioritized, unfunded requirements
- Coordinate requirements with appropriate solutions
- Coordinate biometrics vision/strategy
- Recommend reprogramming of resources
- Develop and coordinate technical analysis of proposed requirements addressing cost, schedule and performance
- Recommend appropriate solutions through JBOCB to JBSESC
- Develop and implement approved solutions

**WGs**

- Working Groups (WGs) discuss topics of importance across the enterprise to include standards, strategy, architecture, requirements, training and policy

**CCBs**

- Change Control Boards (CCBs) discuss changes to biometrics systems such as databases and collection devices

**BIOMETRICS COLLABORATION FORUM**
A core function of the BIMA DoD is to engage stakeholders to better anticipate and assist in meeting warfighter biometrics requirements. In January 2010, the BIMA hosted the first-annual DoD Biometrics Collaboration Forum. Designed to encourage the participants to collectively address urgent issues concerning the DoD use of biometrics, 300 attendees from the DoD and other agencies discussed topics focused on enemy and friendly identification operations and architecture. Friendly-force biometrics sessions made apparent to key audiences that biometrics is a mission enabler in a variety of DoD applications. Participants developed initiatives that they will work toward and report on throughout the year. The agenda was structured to facilitate planned and impromptu collaboration between the attendees and covered a variety of important topics. The 2011 DoD Biometrics Collaboration Forum agenda will feature several of the same ongoing issues, as well as new areas of focus.

# MAJOR ACCOMPLISHMENTS DURING FY10

## IDENTIFY THE INDIVIDUAL

By successfully collecting, storing, matching and sharing biometrics data, an individual's identity can be verified against who he claims to be. The use of biometrics strips away anonymity and enables operators to take action and mitigate tactical, operational or strategic threats. Biometrics capabilities also quickly and precisely verify individuals in support of secure and facilitated business functions.

### DoD Automated Biometric Identification System (ABIS)

The BIMA operates and maintains the DoD ABIS, which provides identity management capabilities for the DoD as well as a means to share biometrics data with other U.S. government and international partners. In FY10, the BIMA provided system engineering, interface control, watch desk and examination services for latent-fingerprint submissions, yellow-resolve cases and multimodal biometrics validation that are vital to the identification process. A yellow-resolve case is a ten-print or facial-image transaction that cannot be handled in an automated fashion within the DoD ABIS but must instead be forwarded to the Examination Services Team for human examination and match determination. The DoD ABIS received nearly 1.3 million submissions in FY10 representing a 25 percent increase from FY09.

The System Engineering team ensured that the DoD ABIS was available 99.5 percent of the time for BIMA customers by monitoring and maintaining more than 200 computers utilizing six operating systems. Additionally, the team monitored and maintained more than 40 databases, 30 functional computing nodes targeting specific biometrics modalities and more than 300 terabytes of storage.

The Interface Control team establishes and maintains interfaces between the DoD ABIS repository and BIMA customers. Interfaces increased by 176 percent, from 42 in FY09 to 116 in FY10. This increase accounts for more than 1,600 individual submitters and reflects a daily increase from approximately 3,000 to approximately 6,000 submissions received as of September 2010, with a projected increase of more than 35,000 submissions per day.

The Watch Desk team provides around-the-clock, year-round services for BIMA customers and in FY10 received more than 25,000 phone calls (a 71 percent increase from FY09), more than 2,500 data requests for information (a 321 percent increase from FY09), more than 105,000 manual cross-domain transfers (a 53 percent increase from FY09), more than 240 special projects (a 129 percent increase from FY09) and more than 8,400 reports (a 119 percent increase from FY09).

The Examination Services team received approximately 55,000 latent-print submissions (reflecting a 62 percent increase from FY09) and more than 63,000 ten-print and facial yellow-resolve cases. These biometrics submissions required more than 1.1 million candidate examinations by a team of 25 examiners and resulted in more than 3,000 latent-print matches, 2,500 latent-to-latent matches and 31,000 ten-print and facial-image matches.

In FY10, DoD ABIS operations enabled latent identifications to approximately 700 improvised explosive device (IED) events and more than 1,300 IED-related watchlist hits. The increase in DoD ABIS customers led to approximately 700 high-value individual captures and 118 denials of U.S. immigration benefits through the Department of Homeland Security (DHS) to date.

## ENABLE THE MISSION

The DoD employs biometrics to enable a range of operational and institutional missions across the spectrum of security, such as high-value individual identification and tracking, personnel recovery, disaster relief, humanitarian assistance, security operations, in-theater interagency operations, U.S. border protection and physical and logical access control.

116th Brigade Combat Team, 29th Infantry Division (Light) Soldiers biometrically enroll an Iraqi Officer at an Entry Control Point in the International Zone, Iraq. (BIMA photo by Mr. Bill Phillips)

## Significant Operational Accomplishments
### 9/11-Related Identifications

The BIMA fosters data sharing and interagency relationships that lead to important identifications. In total, three significant 9/11-related identifications have been made, two of which occurred in FY10. In one such case, a latent fingerprint from evidence collected at a location believed to be a planning site for the 9/11 attacks was matched to a GTMO detainee.

In another case, the BIMA positively identified a latent fingerprint developed on items seized from locations associated with the 9/11 suspects. The subject identified is currently on the Federal Bureau of Investigation (FBI) Most Wanted list. This identification is the first hard evidence to support the suspicion that he was involved with the 9/11 attacks.

## Support to Guantanamo Bay (GTMO) Cuba

Sharing biometrics data with international and coalition partners enables the targeting, tracking and prosecution of known or suspected adversaries.

The BIMA collaborated with international and coalition partners, such as the United Kingdom's New Scotland Yard, and successfully matched biometrics received to DoD biometrics records for former GTMO detainees. The BIMA continues to build these relationships to enhance the ability to protect the U.S. and its partner nations.

Continued efforts centered on the GTMO mission have reconciled detainee records and supported several special projects that have a direct impact on the warfighter. In June 2010, a

Marine SGT Nick Bender conducts an iris scan of an Afghan village elder's eye during a cordon and search mission Feb. 9, in Farah province, Islamic Republic of Afghanistan. The Marines use the BAT to identify Afghans by using fingerprints and iris scans. Bender is the Company-Level Intelligence Cell chief with Company I, 3rd Battalion, 8th Marine Regiment (Reinforced), the ground combat element of Special Purpose Marine Air Ground Task Force - Afghanistan. The SPMAGTF-A mission is to conduct counterinsurgency operations with a focus on training and mentoring the Afghan national police. (Source: Public Intelligence)

mobile support team from the BIMA deployed a new biometrics collection system to the Joint Task Force (JTF) in GTMO to support detainee biometrics collections.  The Biometric Enhanced Enrollment System Transportable equipment was created and deployed in response to requests to provide an all-inclusive, stand-alone biometrics collection system.

**Continuing Support to Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF)**

The BIMA supported the U.S. Forces Iraq efforts to enable the Iraqi government with biometrics by providing equipment for Iraqis to use under U.S. supervision.  The BIMA also provided biometrics data, as requested, to enable the Iraqi Government to continue to develop its own biometrics capability and thus enable the responsible withdrawal of OIF forces from Iraq.

The BIMA continued to support the COCOMs — including planning and executing U.S. Central Command (CENTCOM) regional security architecture — and led international engagement with foreign militaries. The BIMA routinely coordinated with the intelligence community and provided back-end identification analysis when needed and established a Liaison Officer position within the Biometrics Cell in the Joint Staff Force Structure, Resources and Assessment Directorate (J-8) Protection Assessment Division (PAD) at the Pentagon.  This allows the BIMA to review biometrics efforts submitted to the J-8 PAD prior to official validation.

The BIMA supported a variety of biometrics initiatives for JTF 435, U.S. Forces Afghanistan and CENTCOM.  Additionally, the BIMA sponsors a bi-weekly secure video teleconference at the Pentagon that connects Task Force Biometrics to all agencies that have biometrics interests including: the Headquarters Army; the U.S. Department of the Interior; the U.S. Army Intelligence and Security Command; the

National Ground Intelligence Center; Project Manager (PM) Biometrics; the U.S. Army Training and Doctrine Command Capabilities Manager at Fort Huachuca; and CENTCOM. In this forum, stakeholders speak directly with the Commander of Task Force Biometrics and receive and exchange pertinent information in a timely manner to directly support the warfighter and address issues and problems.  In a recent collaborative effort, Task Force Biometrics, JTF 435 and elements of law enforcement provided the framework for an Afghan Ministry of the Interior visit to the U.S.  Additionally, senior members of the Afghan Criminal Investigation Department visited FBI headquarters and the Pentagon, as well as the FBI Criminal Justice Information Services and DoD ABIS facilities, and demonstrated how DoD and law enforcement agencies work together to achieve mission success.

**Port of Entry (POE) Enrollers**

The BIMA provided contract personnel to execute biometrics enrollment missions at critical POE sites into Iraq and Afghanistan. These POE sites are the first line of defense against infiltration of those countries by terrorists.  With U.S. conventional combat operations coming to an end in Iraq, the POE sites provide the most robust biometrics collection opportunities.  Enrollers in Afghanistan supported a number of missions in addition to the POE missions, including biometrically enrolling Afghan Security Force personnel, armed contractor employees and prison inmates. These missions play a key role in the overall Biometrics Campaign Plan for the International Security Assistance Force (ISAF) Commander.

**North Atlantic Treaty Organization (NATO) Collaboration**

Throughout FY10, the BIMA supported efforts in Afghanistan to ensure biometrics requirements were met according to schedule. The BIMA was instrumental in introducing and incorporating biometrics capabilities into NATO future

operations, which resulted in biometrics ranking ninth on the NATO 50-item priority list. In an interoperability effort, the BIMA also supported NATO and ISAF leadership to establish international biometrics information sharing agreements by identifying and researching U.S. and Coalition partner privacy laws and national caveats. The BIMA directly addressed warfighter needs by supporting the development of a number of data-sharing agreements such as these, and by developing a new plan to best engage the COCOMs.

**As-Is Biometrics Enterprise Architecture (EA)**
Over the past year, the BIMA developed and delivered a complete As-Is EA for the DoD biometrics community, and a plan to use the EA as an analytical framework for decision support.

The EA establishes a foundation on which to develop, maintain and mature biometrics-related operations for the DoD Biometrics Enterprise. It helps create a family of systems by institutionalizing and establishing a federated DoD biometrics architecture that promotes consistency through data accessibility.  Through clearly-defined data entities and standards, it also facilitates interoperability across the Enterprise and provides a structured approach for assessing and enforcing compliance to those technical standards and data models.  To that end, the EA provides an analytical framework and insight to enable informed decision making across the Enterprise.

**Excellence Through Technology**
The BIMA recognized that commercial-off-the-shelf (COTS) components provide a means to rapidly introduce new technologies.  Using COTS components in deployed biometrically enabled systems is becoming commonplace due to shrinking budgets and rapid evolution of biometrics technology.  As a result, the BIMA created and published the first BIMA-Certified Products List in FY10.  For the sixth straight year, it exceeded its goal for the number of systems and COTS biometrics technologies evaluated for functionality, standards conformance and integration with the DoD ABIS.

## BIOMETRICS ENTERPRISE GOALS

- 1.0 MILITARY OPERATIONS
- 2.0 BUSINESS FUNCTIONS
- 3.0 INSTITUTIONALIZATION
- 4.0 UNITY OF EFFORT

## ENTERPRISE ARCHITECTURE GOALS AND BENEFITS

**Family of Systems**
- Enable Federation
- Support Joint Capabilities Integration and Development System
- Promote and enable reuse
- Use as baseline for development/change

**Interoperability**
- Facilitate exchange of data
- Synchronize disparate systems
- Manage complexity

**Decision Support**
- Assess and manage risk
- Optimize resources
- Improve effectiveness and agility
- Lower cost

The BIMA employs a three-phased approach to accessing COTS and government-off-the-shelf components for consideration into the BIMA-Certified Products List. These phases include selection, technology assessment in a lab environment and technology assessment in an operational environment. As a result of this testing, the BIMA recommended that the DoD transition to an electronic capture and submission of fingerprints in the background investigation process, which the DoD aims to complete by December 31, 2013. The BIMA laid the groundwork for the inclusion of ten-print fingerprint live-scan scanners on the Army Computer Hardware, Enterprise Software and Solutions Program, the Army Desktop and the Mobile Computing-2 vehicle.

Once fully implemented, DoD stakeholders will be informed by a centralized database of validated, appropriately priced biometrics capabilities for U.S. government applications. These capabilities are certified to be interoperable with the FBI Integrated Automated Fingerprint Identification System and the DoD ABIS. This procurement mechanism will promulgate the use of automated electronic fingerprint devices and will speed fingerprint capture, submission and processing times while providing higher-quality images.

The BIMA also participated in developing the requirements for the Biometric Automated Toolset (BAT) technical refresh conducted by PM Biometrics. Coordination with the Defense Intelligence Agency resulted in a revision to the classification codes used in the BAT, which benefits the biometrics collectors by limiting the amount of information that must be classified and protected as such.

**Testing and Evaluation**
BIMA engineers planned, completed, analyzed and reported on 35 separate events in support of the U.S. CENTCOM, Program Manager

## DoD BIOMETRICS SCIENCE & TECHNOLOGY COMMUNITY



Currently tracking 34 active Biometric Science & Technology projects across the DoD
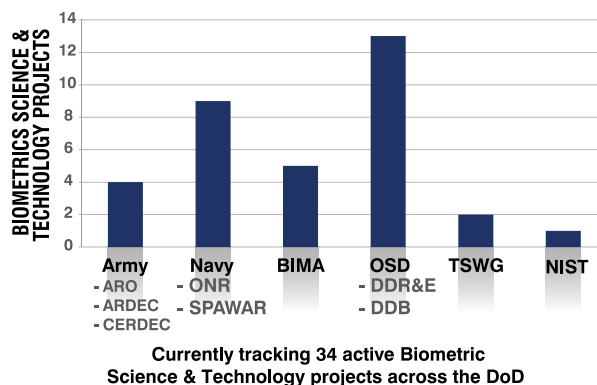
## CURRENT BIOMETRICS SCIENCE & TECHNOLOGY PORTFOLIO



Current Biometrics Science & Technology Projects by Modality
*Ht / Wt Variables   **Gait / Human Movement
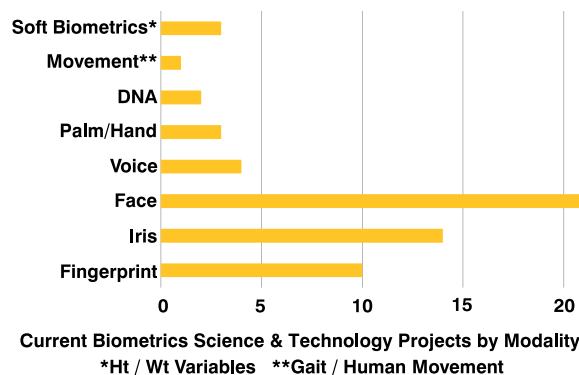
Army Space Program Office, Naval Innovation Laboratory, Army G-2 and others. BIMA involvement contributed to the deployment of more than 2,500 new biometrics pieces of equipment to support OEF and OIF, met user needs and shared data with the DoD ABIS and other databases.

In FY10, the BIMA established an evaluation strategy, methodology and criteria to review biometrics technologies selected for Broad Agency Announcement (BAA) and Biometric Technology Demonstration (BTD) funding. BTDs are funded by the BIMA and are intended to address an identified gap by demonstrating

a biometrics capability in an operational environment.  While similar, the BAA is intended for academia, industry and government (i.e. non-DoD) labs to offer biometrics technology and solutions.  The evaluation strategy monitors progress of each BAA and BTD through close coordination with the DoD sponsor to determine its readiness for deployment. The BIMA worked to synchronize the Biometric Science and Technology efforts across the DoD, as depicted in the charts on page 13.

The BIMA also developed the organization's first institutionalized conformity assessment program by creating the Biometrics Standards Conformity Assessment Program (BSCAP).  The BSCAP is composed of BIMA Test and Evaluation facilities, workforce, policies and procedures required to achieve and sustain compliance and conformance to standards mandated in the DoD Information Technology Standards Registry.   It will serve to identify and improve interoperability, scalability, effectiveness and efficiency of DoD biometrics data repositories and facilitate the net-centric capabilities of the warfighter and DoD biometrics operations.

### Strategic Planning
The BIMA developed an Enterprise Strategic Planning Process to enable stakeholders to collaborate on establishing and executing Enterprise-wide goals.  As part of this process, the Strategic Planning Working Group reconvened this year and reviewed, validated and updated the BESP given the changes in the strategic environment and national and DoD priorities.  The EXCOM will review and approve the recommended BESP updates.

### Biometrics Doctrine
In FY10, the BIMA started analyzing joint doctrine and identifying areas where biometrics could be incorporated.  In coordination with Joint Forces Command, the BIMA reviewed publications and made recommendations to integrate biometrics into doctrine across the spectrum of operations. This allowed lessons learned and best practices for biometrics to be included in the revision process for several Joint Publications (JP), most notably Counter-Improvised Explosive Device Operations (JP 3-15.1), Detainee Operations (JP 3-63) and Stability Operations (JP 3-07).

### Biometrics Standardization and Toolsets
The BIMA was recognized by the DoD Security, Information Assurance, and Cryptography Group for its expertise in Biometrics Standardization. The BIMA chaired the Biometrics Focus Group on behalf of the DoD and provided a forum to make recommendations on the formal adoption of biometrics standards to the DoD Information Technology Standards Registry, the authoritative central repository.  The BIMA made significant enhancements in FY10 to the face and fingerprint image quality measurement tools, which are driven by DoD operational needs and requirements.  The enhancements are used to predict matching accuracy and increase the quality of biometrics samples.

### Requirements Management
BIMA efforts increased COCOM participation in the FY10 quarterly Program Management Reviews (PMRs), which in turn led to biometrics data sharing with countries throughout these commands' areas of responsibility.  Additionally, the BIMA participated in two DoD-led Analysis of Alternatives Studies for the Biometrics Enabling Capability and Tactical Collection Devices, which provided strategic direction for the future Programs of Record.  Along with the Personnel Identification Integrated Capabilities Development Team, the BIMA provided oversight for the current staffing of the Biometrics Enabling Capability and Joint Personnel Identification Version 2 Capabilities Development Documents across the DoD Biometrics Enterprise.

## BIOMETRICS TRIAD



**DoD ABIS**
Stores biometrics from:
- FNs requesting access to U.S. installations overseas
- Latent prints from IEDs and other hostile actions
- Enemy combatants
- Detainees

- Searches biometrics files
- Shares pointers to associated info on match

**DOJ/FBI IAFIS**
Stores biometrics from:
- Arrested individuals
- Criminals and criminal history
- Latent prints from crime scenes

- Searches biometrics files
- Shares pointers to associated info on match

Action:
- Prosecute/exonerate
- Allow/deny access
- Detain/release
- Add/remove from watchlist

- Searches biometrics files
- Shares pointers to associated info on match

**DHS/DOS IDENT**
Stores biometrics from:
- Visa applicants (DOS-BioVisa)
- Visitors to the U.S. (U.S.-VISIT keeps track of entry/exit of visitors appvd in BioVisa)
- Illegal border crossers
- Immigration violators

### Biometrics Triad

The 9/11 Commission, the Markle Foundation and the Government Accountability Office emphasized the need to identify and resolve barriers to information sharing.  Improved access to information and its efficient use is the cornerstone of the nation's ability to protect and defend itself.  As a result, the BIMA actively leads the DoD effort to solidify the Biometrics Triad. The Triad is the graphical depiction of the intended end state for all biometrics information sharing between the three major U.S. government agencies operating large-scale biometrics databases — the DoD, DHS and Department of Justice (DOJ).  In support of the Office of the Under Secretary of Defense for Policy, the BIMA works to ensure interoperability between the DoD, DHS and DOJ.  On September 10, 2009, the DoD and FBI signed a Memorandum of Understanding to share unclassified biometrics and other IdM information in support of the National Security mission.  This interoperability completed one leg of the Biometrics Triad, and with the DHS ability to share biometrics data with the FBI, the second leg of the Triad is complete.

### Biometrics Training Initiatives

In FY10, the BIMA led the Biometrics Training Working Group, a collection of agencies working together to improve predeployment training in biometrics.  BIMA's efforts have ranged from expanding available training and refining training guidance from CENTCOM and U.S. Army Forces Command, to creating a training webpage on the BIMA website that communicates available biometrics training.

**BIMA Central**

The organization launched BIMA Central in FY10, providing a suite of integrated tools to facilitate internal BIMA communication and collaboration, making it easier to share and contribute information through blogs, wikis, forums and document processing. This internal portal allows agency personnel to create and edit documents and content, as well as manage workflow in a collaborative environment through a single point of access, thus supporting the Biometrics Enterprise.

**PROTECT INFORMATION/IDENTITIES/PEOPLE**

In support of the National Security Strategy, the biometrics capability protects people and installations worldwide. The BIMA must also ensure that biometrics data and other associated identifiable information are protected while collecting, storing, matching and sharing.

**Identification-based Decision Process to Enable Confident Transactions (IDProTECT)**

In FY10, the BIMA transitioned the IDProTECT Biometric Identity Management (BIdM) capability into the laboratory environment. IDProTECT evaluates DoD business function applications, such as physical and logical access control and personnel vetting, to one day provide a friendly force biometrics repository. This capability will support two demonstrations starting in 1QFY11, the largest of which is for the Under Secretary of Defense for Personnel and Readiness. In this capacity, IDProTECT will demonstrate a baseline capability that enables Homeland

Security Presidential Directive-12 compliance across the DoD. IDProTECT will also enable the U.S. Army Recruiting Command (USAREC) to expand an operational live-scan capability that better determines whether applicants are eligible for enlistment in the Army or Army Reserve. By employing biometrics capabilities, the USAREC expects to save more than 152,000 days per fiscal year in the pre-screening process for recruits. The USAREC will be able to reject all permanently disqualified applicants and identify applicants requiring waivers prior to expending funds for processing.

**Privacy**

To ensure that all federal databases containing private information are protected from theft, misuse or loss, each federal agency must meet specific legal and federal requirements established in the Privacy Act, the e-Government Act, Office of Management and Budget Memoranda, and other guiding documents on Fair Information Practice Principles.

While operating and maintaining IdM systems, the BIMA protects an individual's personal information against unwarranted privacy invasions. The legal rights of individuals, as guaranteed by all federal laws, regulations and policies, are protected during collection, storage, use or dissemination of biometrics data. BIMA personnel complete training and meet other DoD privacy-related laws, regulations and other guidance.

U.S. Army SPC Michael Gerhart, center, uses a HIIDE system to record the biometrics data of an Afghan man during a patrol in the Zabul province of Afghanistan June 29, 2010. Gerhart is from 2nd Platoon, Delta Company, 1st Battalion, 4th Infantry Regiment. (DoD photo by SSG William Tremblay, U.S. Army)

Global Entry kiosks located in airports throughout the nation capture travelers' biometrics information to verify their identities. Photo courtesy of U.S. Customs and Border Protection.

# WAY AHEAD

The BIMA leads the way into future challenges as biometrics capabilities continue to make a positive impact on the war efforts in Afghanistan. Many BIMA DoD stakeholders will focus on more types of biometrics applications in support of national security, such as disaster relief, border security and other peacetime operations. Biometrics technologies are key enablers in efforts to protect the nation, its citizens and its interests across the spectrum of security. Biometrics identity capabilities can also help enable and transform business applications to protect information and facilitate the conduct of business processes. There is no doubt that FY11 will be another year of great strides.

**To-Be Biometrics Enterprise Architecture (EA)**
Using the delivered As-Is Biometrics EA as a baseline, the BIMA is developing an interim To-Be DoD Biometrics EA covering 2015 and beyond that is scheduled to be released in December 2010. The 2015 Biometrics EA will provide enduring biometrics capabilities for the DoD and its mission partners to enable IdM. The core capabilities will remain the same — collecting, storing, matching, managing, analyzing, referencing and sharing biometrics — and will support of a variety of mission sets including access control, intelligence, warfighting, law enforcement, emergency response and disaster relief.

**Interagency Collaboration**
Interaction with interagency partners is paramount to maintaining and expanding the BIMA ability to determine the intent of unknown persons, secure borders and cooperate with foreign partners to deny the enemy freedom of maneuver and safe haven. National Security Presidential Directive 59 requires "agencies

to use, in a more coordinated and efficient manner, all biometrics information associated with persons who may pose a threat to National Security, consistent with applicable law, including those laws relating to privacy and confidentiality of personal data." To this end, the BIMA will continue to initiate and support biometrics sharing agreements with DoD components and support DoD efforts to form agreements with the Department's interagency partners.

**DoD Identity and Privilege Management (IPM)**
Identity and Privilege Management (IPM) minimizes cybersecurity intrusions by maintaining continuity of operations, maximizing force protection and facilitating continuity of government. The BIMA represented BIdM stakeholders in publishing the 1QFY11 DoD Biometrics Enterprise IPM Recommendations. A document on how the DoD will implement those recommendations and guidance will be developed in FY11.

This initiative ensures an integrated and interoperable implementation of biometrics in support of IPM, as the pace of biometrics adoption is increasing rapidly across the government, DoD and commercial arena.

**Improving Systems Efficiency**
The BIMA will further improve biometrics systems efficiencies in FY11 and beyond by increasing Random-Access Memory space and throughput and by more effectively managing transactions. The BIMA will also improve the algorithms for current capabilities such as facial features, finger and palm prints, and iris patterns. Other modalities are also being explored, such as voice and the DNA link to current biometrics.

## Enhance DoD Business Functions

Biometrics can establish greater levels of trust for routine DoD business functions, the processes and systems by which to develop and sustain operational forces, as defined by U.S. Code, Title 10. Biometrics can be applied to Human Resource Management, Health Services, Installation Management, Legal Affairs and Resource Management. The BIMA will publish a draft Biometrics Business Functions Framework (BBFF) in FY11, which will help decision makers incorporate biometrics into DoD business functions by providing guidance on policy implications, best practices and planning. It will be designed as a living document that will enable the Enterprise to leverage lessons learned from BIMA-documented experiences in which biometrics are employed in support of DoD business functions.

## Continuous Requirements Management

In FY11, the BIMA will continue to institutionalize biometrics within the DoD. The BIMA will utilize the Biometrics Requirements Working Group to track and address common biometrics initiatives and as part of the Biometrics Governance Forum, will seek to resolve challenges at the lowest level and provide senior leadership with timely information. Additionally, the BIMA will provide the Biometrics Governance Forums with results of its quarterly PMR cycle.

## Continuous Strategic Planning

The BIMA will continue efforts to implement an Enterprise-wide, continuous strategic-planning cycle to guide the evolution of the DoD Biometrics Enterprise. In FY11, the BIMA will conduct quarterly In-Progress Reviews (IPRs) for the BESP and I-Plan through the governance bodies to include enterprise stakeholders who own BESP objectives. The IPRs will serve as a platform for recommending changes and updates to the BESP and I-Plan, while reporting the status of performance metrics and progress against the action plans.
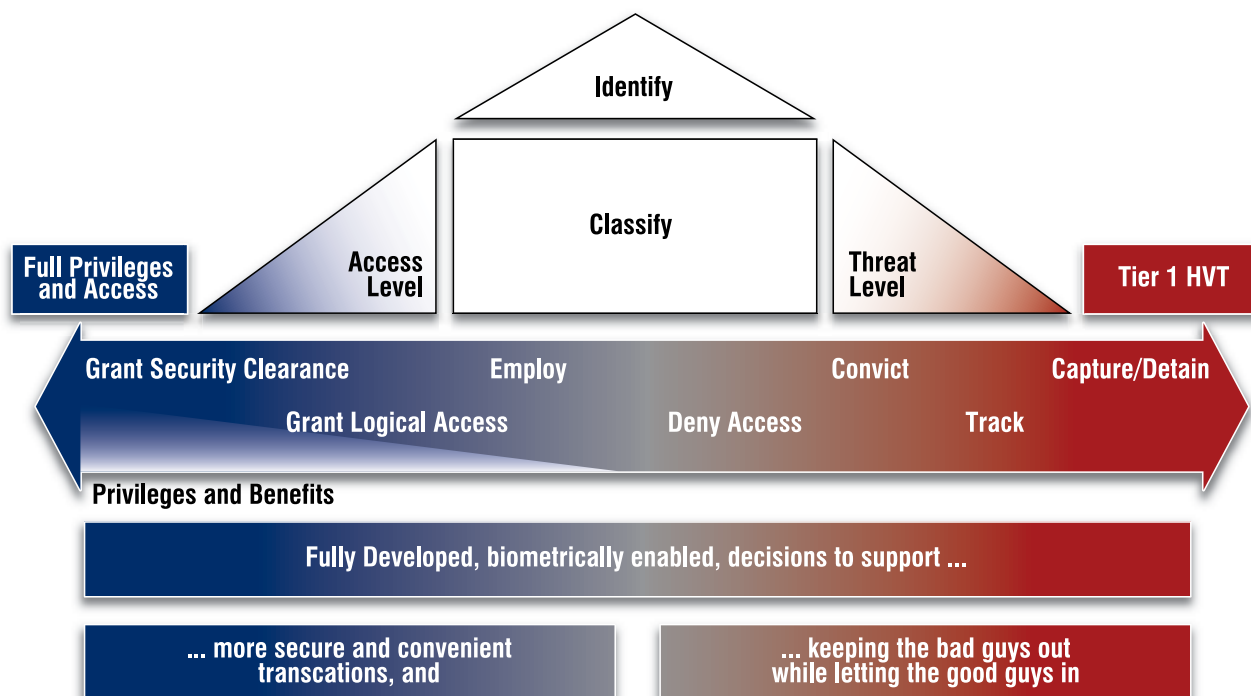
Finger vein technology as used for secure access to an ATM. (Source: flickr/Matsuyuki)

# CONCLUSION

"Our organization is focused on providing the enabling capabilities of biometrics to the DoD, other government agencies and to our international, state and local partners."

— Dr. Myra S. Gray, Director and Executive Manager, DoD Biometrics
Excerpted from interview in "Findbiometrics.com," February 1, 2010

The nation requires innovative methods to strip away the anonymity of adversaries, verify identities and detect threats. Security challenges reside not only abroad, but also at home and in the conduct of daily business. Biometrics capabilities can make business processes more secure while enhancing efficiency and timeliness. Biometrics is a key enabler in combating terrorism and other threat-related activities. As OIF draws to an end, biometrics continues to make a difference in OEF in achieving warfighting mission success. The BIMA implementation of the ABIS and its role in biometrically enabled intelligence has created a greater awareness of biometrics overall.

The BIMA has made significant steps toward realizing full interoperability between the DoD, DOJ and DHS. By collaborating with international partners, many successful matches have been made to the DoD biometrics records of adversaries. There is also an extraordinary potential for biometrics applications with DoD institutional and business operations. With the initial draft of the BBFF in FY11, the BIMA will assist decision makers regarding the applications of biometrics in business functions by providing guidance on policy implications, best practices and planning.

Enabling critical DoD military operations and business functions while protecting and sharing biometrics data is the embodiment of Identify, Enable, Protect.

A U.S. Soldier with Blackwatch Company, 2nd Battalion, 1st Infantry Regiment, collects biometrics data from a village elder in Hutal, Afghanistan, March 23, 2010.
(U.S. Air Force photo by SSG Dayton Mitchell)
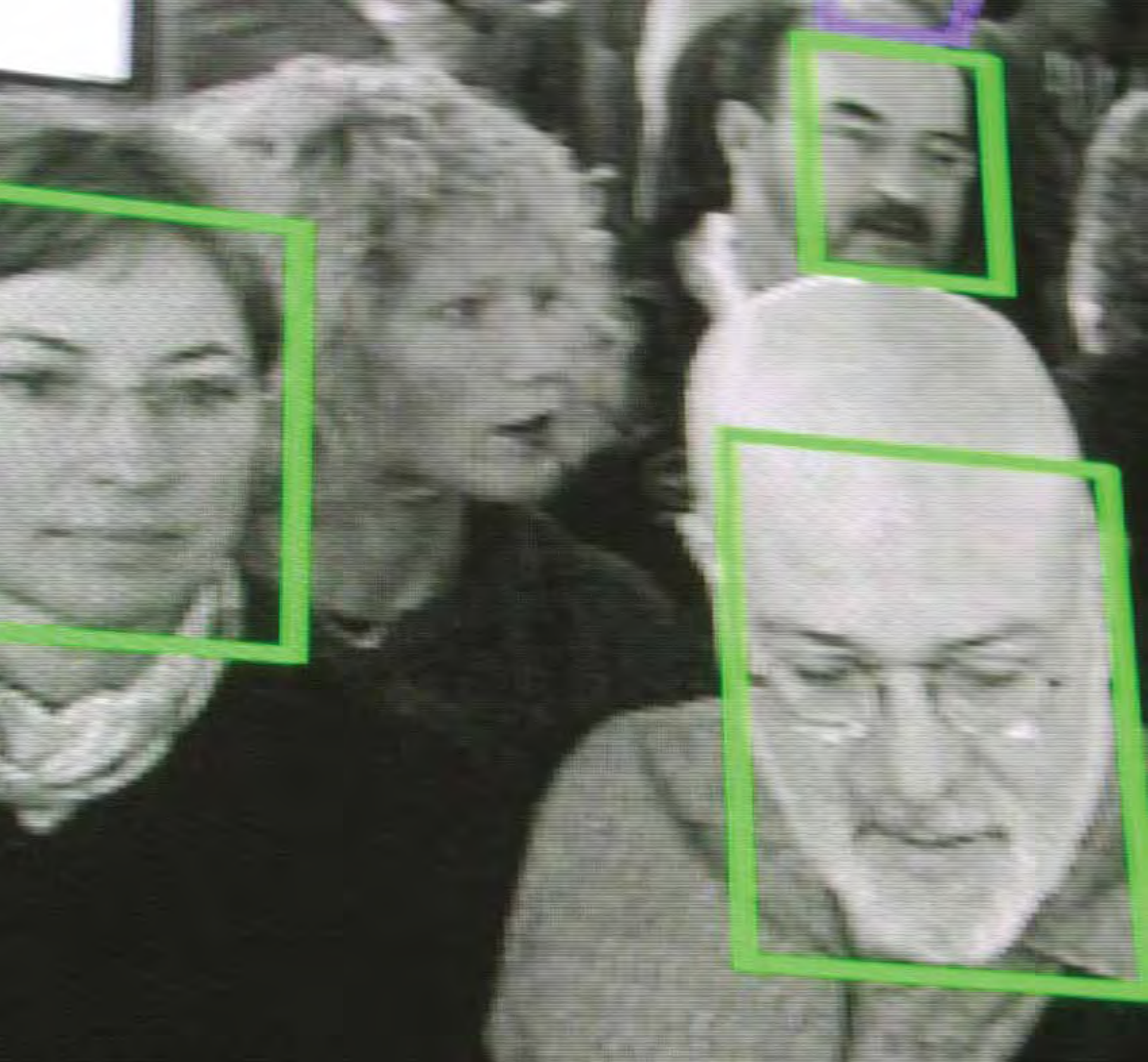
Face recognition system locating multiple faces in a crowd. (Source: Mediamatic/KentKB)

# ACRONYM LIST

| | | | | |
|---|---|---|---|---|
| **ABIS:** | Automated Biometric Identification System | | **FY:** | fiscal year |
| **BAA:** | Broad Agency Announcement | | **GTMO:** | Guantanamo Bay |
| **BAT:** | Biometric Automated Toolset | | **HIIDE:** | Handheld Interagency Identity Detection Equipment |
| **BBFF:** | Biometric Business Function Framework | | **IED:** | improvised explosive device |
| **BESP:** | Biometrics Enterprise Strategic Plan | | **IDProTECT:** | Identification-based Decision Process To Enable Confident Transactions |
| **BIdM:** | Biometric Identity Management | | **IPM:** | Identity and Privilege Management |
| **BIMA:** | Biometrics Identity Management Agency | | **IPR:** | In-Progress Review |
| **BSCAP:** | Biometrics Standards Conformity Assessment Program | | **ISAF:** | International Security and Assistance Force |
| **BTD:** | Biometric Technology Demonstrations | | **J-8:** | Joint Staff Force Structure, Resources and Assessment Directorate |
| **BTF:** | Biometrics Task Force | | **JBOCB:** | Joint Biometrics Operational Coordination Board |
| **CENTCOM:** | U.S. Central Command | | **JBTCB:** | Joint Biometrics Technical Coordination Board |
| **CCB:** | Change Control Board | | **JTF:** | Joint Task Force |
| **COTS:** | commercial off-the-shelf | | **NATO:** | North Atlantic Treaty Organization |
| **COCOM:** | Combatant Command | | **OEF:** | Operation Enduring Freedom |
| **DHS:** | Department of Homeland Security | | **OIF:** | Operation Iraqi Freedom |
| **DoD:** | Department of Defense | | **PAD:** | Protection Assessment Division |
| **DoDD:** | DoD Directive | | **PM:** | Project Manager |
| **DOJ:** | Department of Justice | | **PMR:** | Program Management Review |
| **DOS:** | Department of State | | **POE:** | Port of Entry |
| **EA:** | Enterprise Architecture | | **USAREC:** | U.S. Army Recruiting Command |
| **EXCOM:** | Executive Committee | | | |
| **FBI:** | Federal Bureau of Investigation | | | |

# STRATEGIC OBJECTIVES INDEX

Approved as of August 27, 2008; updates in progress.

Peripheral optical fingerprint device scanning user's thumb for network access. (© iStockphoto/N_design)