



Protect the nation through the employment of biometrics capabilities.

Biometrics provide the solution with a three-step capability:

Identify/Enable/Protect. **Identify** strips adversaries of their anonymity. **Enable** describes the functions possible with biometrics, from compiling watch lists of terrorists to enabling base access for individuals. **Protect** is the payoff – to protect information, identities, people, and installations worldwide.





Biometrics are “measurable physical and behavioral characteristics that enable the establishment and verification of an individual’s identity.”

- Capstone CONOPS for DoD Biometrics, November 2006.



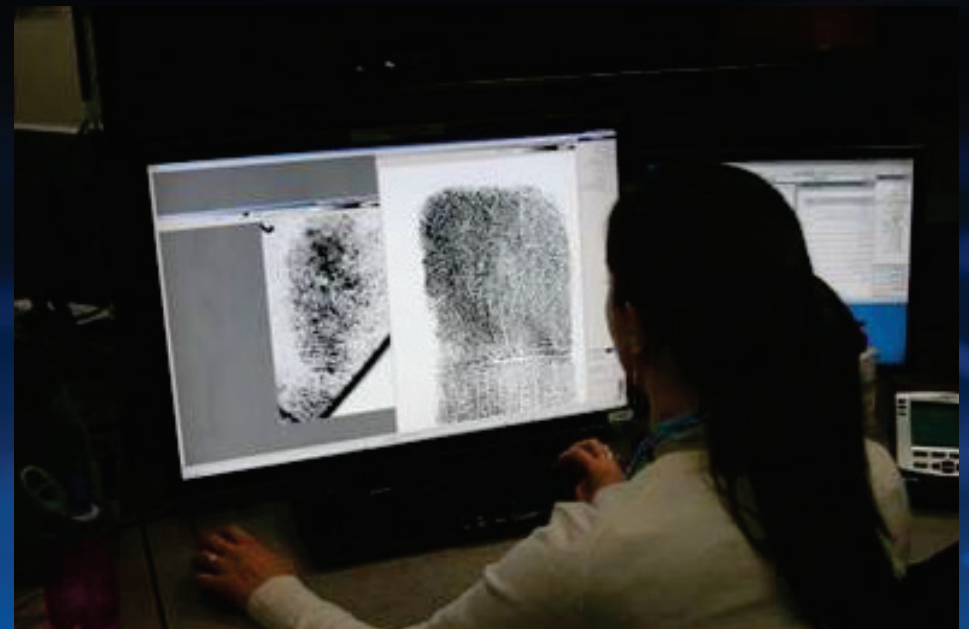
Located in Crystal City, VA, and Clarksburg, WV, the **BIMA** operates through the Executive Agent authority given to the Secretary of the Army and delegated through the G-3/5/7.

Since July 2000, the organization has collaborated at the task force level and now at the agency level with a variety of stakeholders and the wider biometrics community to empower the warfighter and buttress national security. What was once a quick-reaction program to address a variety of identity challenges is maturing into an enduring capability.



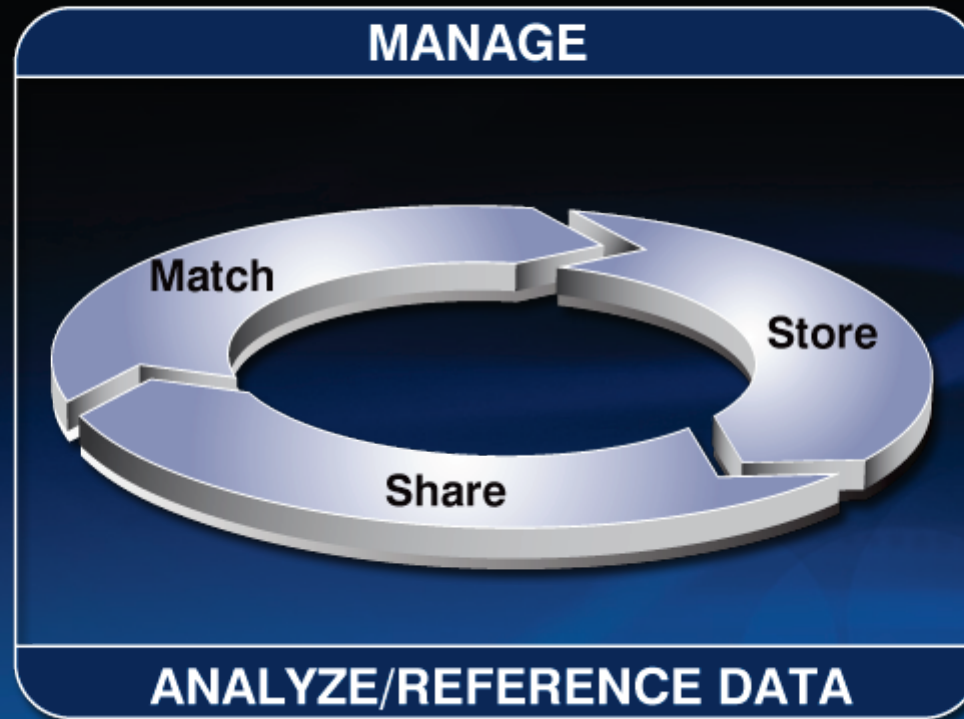


The **DoD Biometrics Enterprise** is an entity made up of the Department's Joint, Service and agency organizations working together to integrate biometrics into the identity transactions needed to support military operations and Departmental business functions. The DoD Biometrics Enterprise mission is to provide enduring biometrics capabilities to the DoD and its mission partners to enable the identification of individuals in support of national security interests.



**Biometric Modalities**

- Fingerprint
- Iris
- Face
- Palm
- DNA
- Voice
- Future Modalities



**Operational Applications**

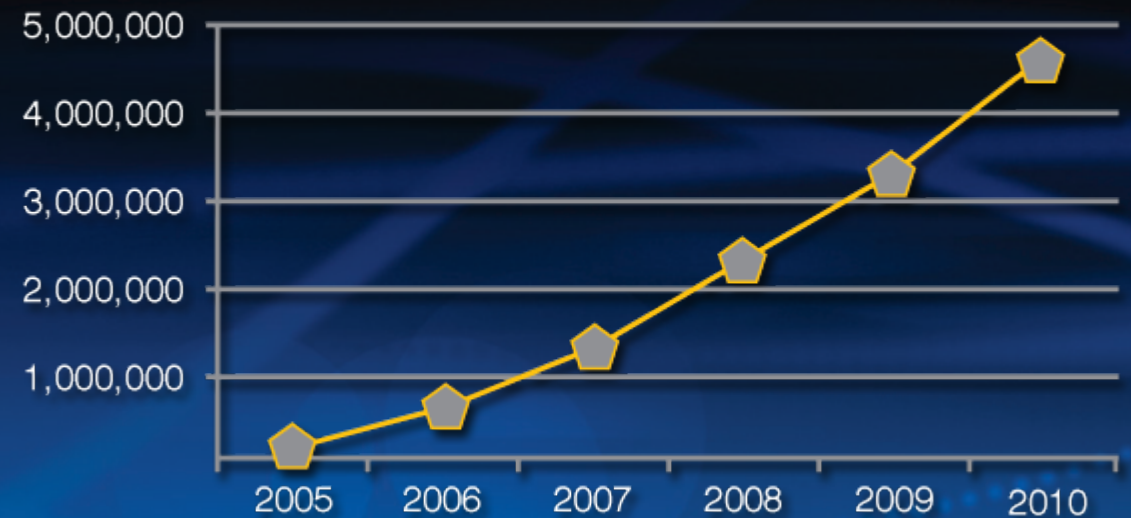
- Populace Management
- Force Protection
- Access
- Surveillance
- Monitoring
- Combat ID

## Automated Biometric Identification System (ABIS)

The DoD ABIS stores and matches biometric data to enable targeting, tracking and prosecution of known or potential adversaries. The DoD ABIS is also the means through which biometric data is shared with other U.S. government agencies.

- + 7 million records
- 6,800+ transactions per day, rated for 8,000
- Latent-to-latent searches
  - 120,000+ latent fingerprints
  - 8,800+ latent matches; 3400 latent-to-latent matches

### Increase in ABIS enrollments over time



Enrollments are increasing 16-39% each year



## DoD Biometrics Priorities

- Afghanistan
- Institutionalize the capability
- Global application of biometrics technologies to support COCOM missions
- Seamless interagency interoperability

## SO WHAT?

### Detainee Operations

- **Attain convictions in criminal courts**
- **2,300 denied early release**

### Defend the Homeland

- **218+ Interdictions in collaboration with interagency partners**

### ABIS Records

- **7 million records in ABIS (4.4 million unique identities)**



## Securing the Border

On May 27, 2011, the BIMA received a submission for an individual who applied for U.S. immigration benefits through the Department of Homeland Security's Refugee Affairs Division. This resulted in a "hit." The individual had been enrolled in the ABIS in October 2004, most likely by a soldier using the Biometrics Automated Toolset (BAT), for stealing evidence from an investigation. The individual had been issued an Interment Serial Number from the National Detainee Reporting Center. His status was Tier 4 (Do Not Hire, Deny Base Access, Disqualify for Police or Army Training). The hit was a significant success for the interoperability of DoD with the Department of Homeland Security.



## Trail of Fingerprints

On July 21, 2011, an enrollment from the U.S. Special Operations Command arrived at the DoD ABIS watch desk in West Virginia. Experts soon determined that the fingerprints matched those already taken from several Improvised Explosive Device (IED) events—the eventual count reached 33 events with 118 latent prints—stored in the DoD ABIS Unsolved Latent File. The information in the file, which had been submitted the prior March by Coalition Forces, had been processed by multiple agencies between May 2010 and July 2011 with no significant identifications until July 21. The watch desk staff responded promptly to SOCOM forces, who detained the individual. This Super Hit, which marked a record number of IED events traced to one individual, demonstrated steady improvement in the BIMA's ability to connect the dots in pursuit of the most elusive and dangerous adversaries.





## On High Seas

On May 15, 2009, U.S. Naval personnel from the USS Gettysburg sent biometric files to the BIMA on 17 suspected pirates enrolled during an encounter in the Gulf of Aden. While this resulted in no “hits” from previous enrollments, each submission grew the tactical value of the ABIS. Moreover, such demonstrations of the Navy’s ability to quickly locate individuals in the database provide an ongoing deterrent to pirate activity.

