IDENTIFY/ENABLE/PROTECT

ANNUAL REPORT

FY11

BIMA BIOMETRICS IDENTITY MANAGEMENT AGENCY

TABLE OF CONTENTS

1 . . . . **Director's Message**

3 . . . . **About the BIMA**
3 . . . . . Mission
3 . . . . . Vision

4 . . . . **Identify, Enable, Protect**
4 . . . . . A Word of Thanks to Our Stakeholders
4 . . . . . Executive Agent (EA) and Executive Manager (EM) for DoD Biometrics
6 . . . . . Strategic Focus

9 . . . . **Major Accomplishments FY11**
9 . . . . . Identify the Individual
9 . . . . . DoD ABIS Ups the Ante
11 . . . . Modern Architecture
11 . . . . Watching for Bad Guys
13 . . . . Conformity
14 . . . . Biometrics and Forensics: A Double Threat
14 . . . . Enable the Mission
14 . . . . Supporting the Warfighter
18 . . . . Technology: Leaning Forward
18 . . . . Interoperability
18 . . . . The Biometrics Triad
21 . . . COCOM Engagement
22 . . . . BITMAP
24 . . . . Requirements Management
27 . . . . Collaboration With Academia
29 . . . . Protect Information, Identities, People
29 . . . . Measuring Success
29 . . . . Privacy
30 . . . . DoD Identity Assurance

33 . . . . **Way Ahead**
33 . . . . The DoD ABIS
33 . . . . EA and EM
33 . . . . Interoperability
33 . . . . Forward-Looking Architecture
35 . . . . Privacy: A High Priority

36 . . . . **Conclusion**
36 . . . . Enduring Capability and Program of Record

37 . . . . **Acronyms**

INSIDE STORIES

7 . . . . . Accuracy is Everything
12 . . . . Higher Standards
15 . . . . The One-Two Punch
19 . . . . Identity Dominators
23 . . . . The Strength in Sharing
26 . . . . Mystery Solvers
34 . . . . High Seas Success

SUCCESS STORIES

11 . . . . Jailbreak
18 . . . . Quick Hits
21 . . . . Looking South
22 . . . . Securing the Border
24 . . . . The Super Hit
31 . . . . The Turban Bomber

U.S. Soldiers with Alpha Company, 1st Battalion, 17th Infantry Regiment use a Handheld Interagency Identity Detection Equipment (HIIDE) biometrics device to record information about an Afghan man in Badula Qulp, Helmand province, Afghanistan, Feb. 12, 2010. The HIIDE is a multimodal biometric system that collects and compares fingerprints, iris scans and facial photos against an internally downloaded biometric watchlist. The Soldiers are participating in Operation Helmand Spider. (U.S. Air Force photo by TSgt Efren Lopez/Released)

DIRECTOR'S MESSAGE

To say that Fiscal Year 2011 has been a positive and exciting one for the Biometrics Identity Management Agency (BIMA) would be an understatement. In my first year as Director, the BIMA continued to play a key role in empowering Department of Defense (DoD) Biometrics. Our central biometric data repository, the DoD Automated Biometric Identification System (DoD ABIS), has steadily increased in the number of records while maintaining its speed and responsiveness for the benefit of the DoD, our interagency partners and international allies.

Our plan for full interoperability with the Department of Homeland Security (DHS) is on schedule, projected for late 2012. Memoranda of Agreement and Cooperation with other organizations during the fiscal year demonstrated that the BIMA possesses unique, multimodal biometric datasets and expertise that no one else has. On Nov. 18, 2011, we placed the final steel beam atop our new Biometrics Technology Center in Clarksburg, W.Va., which will be ready for occupation in FY14. This amazing facility, which we will share with the FBI's Biometric Center of Excellence, reflects the DoD commitment to jointness in our efforts to secure the nation.

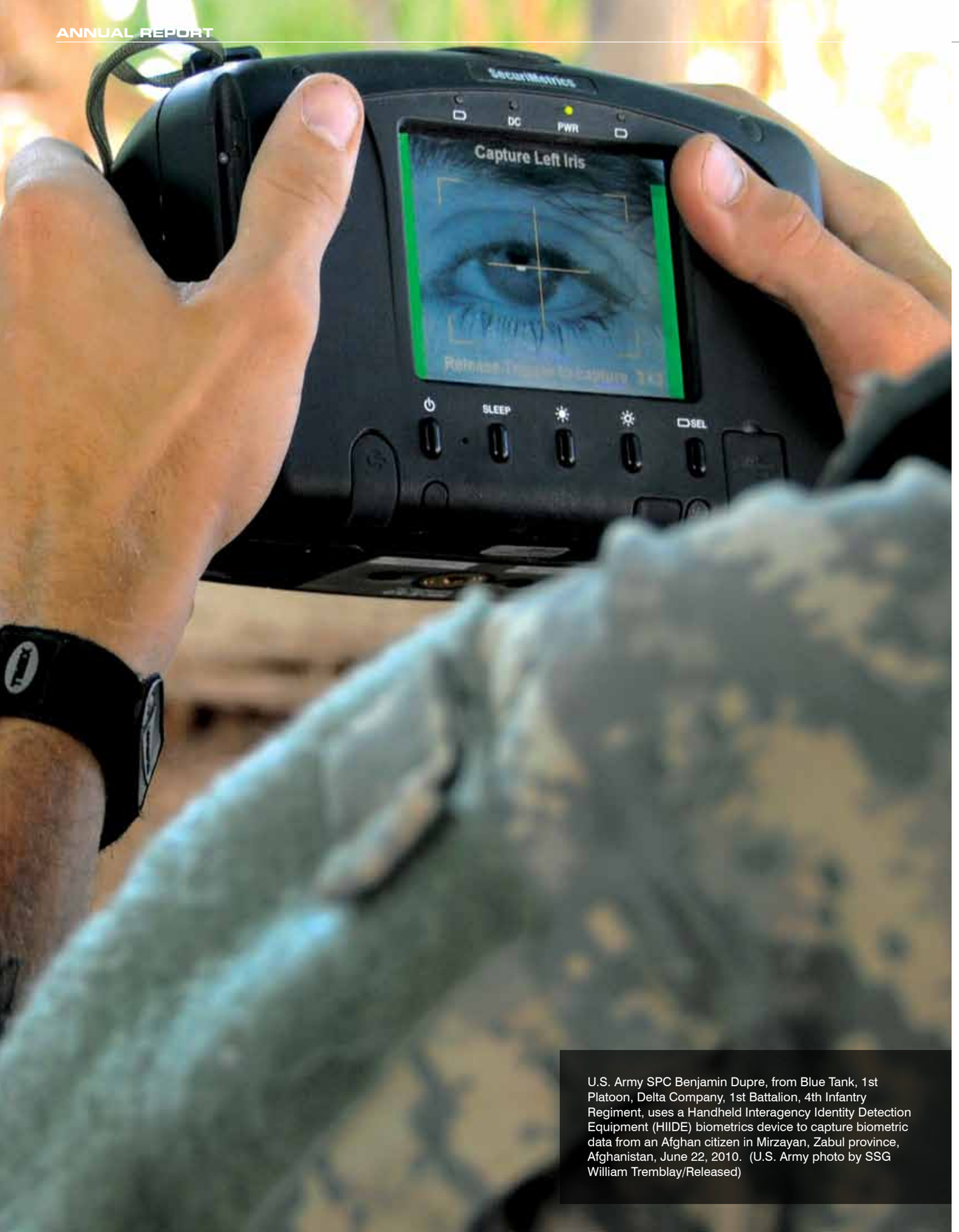
In this war that we've been conducting for the last decade, as in other wars, specialized capabilities have evolved to support the fight. Biometrics is one of them. Biometrics let us identify whom we need to deal with on the battlefield, and help us take those individuals off the battlefield.

But that's not the only role for biometrics, which will endure in terms of the DoD's business operations. There's an increasing demand — broadly, not just in the DoD — to know who an individual is who's asking for certain privileges, or for access to certain services. Biometrics offer a tool that enables us to appropriately provide that access with assurance. And that's why biometrics has to endure as a capability. We cannot put it on a shelf and bring it back out the next time we go to war.

It is true that, at a time when improvements in biometrics technologies and capabilities are accelerating, a period of fiscal austerity looms. This will be felt throughout the DoD and the entire United States government. As decision makers reshape the future of many programs, I believe that biometrics will remain an enduring capability and potentially become a program of record.

I look forward to the challenges and achievements of the coming year. Please join me in my optimism about the future of our biometrics work, and in my gratitude to all in the biometrics community who safeguard our national security.

Sincerely,
Dr. Thomas Killion



U.S. Army SPC Benjamin Dupre, from Blue Tank, 1st Platoon, Delta Company, 1st Battalion, 4th Infantry Regiment, uses a Handheld Interagency Identity Detection Equipment (HIIDE) biometrics device to capture biometric data from an Afghan citizen in Mirzayan, Zabul province, Afghanistan, June 22, 2010. (U.S. Army photo by SSG William Tremblay/Released)

ABOUT THE BIMA

MISSION:
The BIMA leads DoD activities to program, coordinate, integrate and synchronize biometrics technologies and capabilities, and to operate and maintain the DoD authoritative biometrics database in support of the National Security Strategy.

VISION:
Protect the nation through the employment of biometrics capabilities.

Biometrics are measurable physical and behavioral characteristics that enable the establishment and verification of an individual's identity. They include:

- Fingerprint
- Facial recognition
- Iris recognition
- Palm print

Biometrics also refers to the process of using automated methods to recognize an individual based on these and other measurable characteristics. Researchers in the field of biometrics also continue to improve the usability and responsiveness of DNA, as well as behavioral modalities such as gait, to better establish identity in specific situations.

IDENTIFY, ENABLE, PROTECT

The problem: **ANONYMITY**

The solution: **BIOMETRICS**

Employing biometrics is a three-step process. The first step, **Identify**, strips adversaries of their anonymity on battlefields, at border crossings and other transit points and within the United States. The second, **Enable**, represents the many functions that U.S. Forces can carry out with biometrics, from compiling watchlists of suspected terrorists to enabling base access for cleared individuals. The third, **Protect**, furnishes the payoff of biometrics. It answers the question of why there's a need to identify and enable — to protect the warfighter, the advantage, the mission and, ultimately, the nation.

A WORD OF THANKS TO OUR STAKEHOLDERS

DoD Biometrics stakeholders include a wide variety of groups. For example:

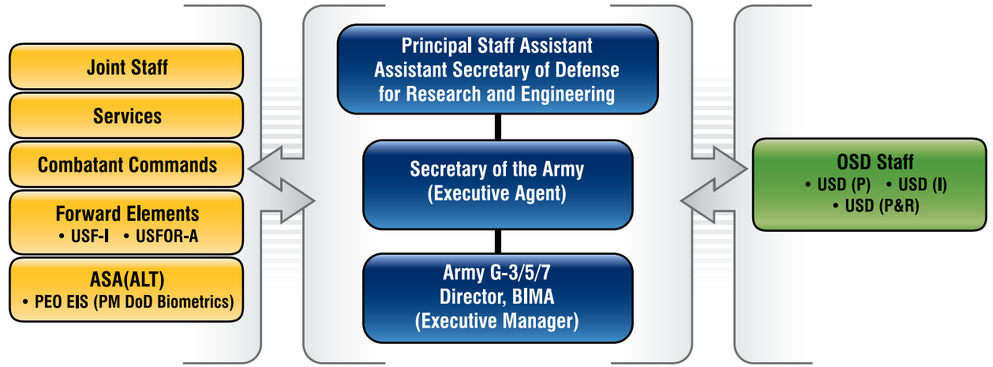
- Soldiers, Sailors, Airmen or Marines on the ground in places like Iraq and Afghanistan send us fingerprints and other biometric data that then provide a match, or "hit," to our databases and watchlists.
- Navy crews operating in international waters rely on our biometric data's ability to pull the cloak of anonymity from modern-day pirates.
- The intelligence analyst fuses biometric matches with contextual information to identify the enemy.
- Our partner agencies include the Department of Justice (DOJ) and DHS, with whom we share biometric data to support national security interests.

A key part of the BIMA mission is to better engage with you, the stakeholder, to anticipate and serve your warfighting and law enforcement needs, and to enable and empower your work.

EXECUTIVE AGENT (EA) AND EXECUTIVE MANAGER (EM) FOR DOD BIOMETRICS

In July 2000, Congress designated the Secretary of the Army as the EA for DoD Biometrics, tasked to "lead, consolidate and coordinate all biometrics information assurance programs of the Department of Defense." The Director, BIMA, is the EM for DoD Biometrics.

DoD BIOMETRICS STRUCTURE



The Principal Staff Assistant (PSA), the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) provides oversight to the EA and EM for DoD Biometrics, who support numerous DoD elements including the Joint Staff, Services and Combatant Commands (COCOMs); Forward Elements including U.S. Forces – Iraq (USF-I) and U.S. Forces – Afghanistan (USFOR-A); and the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)), including the Program Executive Office Enterprise Information Systems (PEO EIS) and the Project Manager (PM) DoD Biometrics. The EA and EM also support the Office of the Secretary of Defense (OSD) and the Under Secretaries of Defense for Policy, Intelligence and Personnel and Readiness.

The agency leads DoD activities to program and synchronize biometrics concepts, technologies and capabilities, and operates the DoD ABIS, the department's authoritative, multimodal biometric data repository. What began as a suite of enabling technologies for such needs as secure access to military installations soon began offering innovative ways to identify and track suspected terrorists. In Iraq and Afghanistan, biometrics have been called upon to help counter the problem of Improvised Explosive Devices (IEDs), tracing fingerprints back to those who make and detonate IEDs. In this way, biometrics have grown from a quick-reaction security measure to an enduring capability.

STRATEGIC FOCUS

In FY11, the BIMA, operating within the Deputy Chief of Staff, G-3/5/7, has continued to serve as a leader in the larger DoD Biometrics Enterprise. The Enterprise consists of the department's Joint, Service and other partners working to integrate biometrics into the identity transactions needed to support military operations and departmental business functions. The mission of the Enterprise is to provide enduring biometrics capabilities to the DoD and its mission partners, and enable identification of individuals in support of national security interests. Operating globally, the Enterprise protects rights and services for partners while denying anonymity to adversaries. The Biometrics Enterprise Strategic Plan (BESP) sets the direction for the Enterprise through the pursuit of four goals:

- **Military Operations** — Meet the warfighting biometric needs of 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.

ACCURACY IS EVERYTHING

CHELEY GABRIEL, BIMA

Chief, Enterprise Operations Division
Clarksburg, W.Va.

"The key to what I look at, being the ABIS manager, is future throughput, capacity and accuracy," says Gabriel, who also has 23 years of active duty, National Guard and Reserve service in the U.S. Army. The DoD Automated Biometric Identification System (DoD ABIS) currently receives about 130,000 enrollments per month. "That tends to grow every quarter by another 5,000 to 10,000," she says. "So that's how we're projecting what our capacity and throughput need to be." But it's about quality, too. For instance, the DoD ABIS receives biometric files from an array of submitters with varying degrees of accuracy. "You hear lots of personnel in the community talk about throughput and capacity, but the accuracy is given a diminished role," Gabriel says. "Looking forward, I want to make accuracy more of a priority for ABIS than it has been. So whether that's better training with our personnel who are in the areas of operation actually using the biometric devices and systems, to talking to the vendors myself to get them to make better and more reliable devices, accuracy is a major goal for the future."

> "Looking forward, I want to make accuracy more of a priority for ABIS than it has been."

U.S. Navy PO2 William Padilla, from the Nuristan Provincial Reconstruction Team Military Police, uses a Handheld Interagency Identity Detection Equipment (HIIDE) biometrics device during a mission in Nurgram district center, Nuristan province, Afghanistan, May 13, 2010. (U.S. Air Force photo by SSgt Steven R. Doty/Released)

MAJOR ACCOMPLISHMENTS FY11

IDENTIFY THE INDIVIDUAL

A threat greater than the enemy you know is the one you don't. The ability to refuse anonymity to an adversary provides a critical advantage. In FY11, the BIMA reached a new level in its ability to collect, match, store, share and manage biometric data, executed with speed and accuracy. The response back to the warfighter has resulted in the prosecution of a wide array of tactical and strategic threats.

DOD ABIS UPS THE ANTE

FY11 was a benchmark year for the DoD ABIS, the authoritative repository of DoD biometric data. The BIMA operates and maintains the DoD ABIS, and in FY11 continued to share data with COCOMs, other U.S. government agencies and international partners. System storage, biometric enrollments, matches, submitters and the overall number of latent, or anonymous, submissions all increased.

On July 28, 2011, BIMA operators surpassed six million total records stored in the DoD ABIS Search Core. By the end of FY11, the database received nearly 1.6 million submissions for the year, a 23 percent increase over FY10, for a total of 6.4 million submissions from new and existing customers. The DoD ABIS offers ever more complete biometric data through the fusion of multiple modalities — fingerprint, iris, palm print and facial recognition — and never sleeps, 24/7/365.

The power of the database complements the power of the BIMA's staff of Biometric Examiners (BEs) and Certified Latent Print Examiners (CLPEs), who employ highly specialized skill sets not easily found — there are fewer than 1,000 CLPEs worldwide. The Unsolved Latent Print File in the DoD ABIS currently contains more than 200,000 files of latent prints such as those recovered from crime scenes or weapons caches. Each latent file must be manually encoded by a CLPE on the Biometric Examination Services (BES) team prior to submission into the DoD ABIS. The database returns a candidate list of matches that must be reviewed by a CLPE to determine if the source of the print can be identified. More than 1 million latent print comparisons are conducted by the team each year. In addition, almost 6 percent of all tenprint submissions (those with prints from all 10 fingers) are sent to the examiners for comparison, amounting to about 14,000 comparisons per month.

The Systems Engineering team maintained a 99.5 percent availability of the DoD ABIS, maintaining more than 300 computers and more than 400 terabytes of storage, encompassing more than 40 individual databases and 30 computing nodes. Beyond the assets for the DoD ABIS, the BIMA's Information Technology (IT) staff managed almost 600 additional servers, databases, operating systems, computing nodes and work stations that provide the IT backbone for the agency.

> "You can present a fake identification card. You can shave your beard off. But you can't change your biometrics."
>
> SGM Robert Haemmerle, U.S. Army, Combined Joint Interagency Task Force 435, Afghanistan
> — *New York Times*, July 13, 2011

The BIMA has the direct responsibility for establishing and maintaining both the technical and administrative aspects of submitters to the DoD ABIS, such as compatibility of submissions to the database as well as security and sharing stipulations, within and outside of the DoD. The agency has a direct role in the establishment of more than 3,400 registered Originating Agency Identifiers (ORIs). ORI registrations, which represent potential new customers, climbed from 1,600 in FY10 to 3,400 in FY11, an increase of 113 percent. As a direct result, the monthly submission rate climbed exponentially by the end of FY11 to 130,000 submissions per month, and continues to rise on average between 5,000 and 10,000 per quarter.

The Watch Desk team, available to customers 24/7, took more than 25,500 phone calls, a 2 percent increase over FY10; 3,100 data requests for information, a 24 percent increase over FY10; 140,000 manual cross-domain transfers, a 33 percent increase; 280 special projects, a 17 percent increase; and produced 8,000 reports for various customers that include information such as daily enrollment numbers, representing a 5 percent decrease after reducing for redundant and obsolete reports.

The BES team received approximately 64,700 latent print submissions, an 18 percent increase over FY10, and more than 98,750 tenprint and facial yellow-resolve transactions, a 57 percent increase over FY10. A yellow-resolve case is a tenprint or facial-image transaction that cannot be handled automatically by the DoD ABIS, and must be forwarded to the BES team for human comparison and match determination. More than 53,000 latent print files were submitted by the BES team. Latent print submissions resulted in more than 4,600 latent print matches, a 53 percent increase over FY10. Of the total latent print matches for FY11, 2,100 were associated with IED-related evidence. Though latent candidate lists were reduced by half as a result of efficiency studies, biometric examinations were still comparable to the prior year, requiring more than 1 million candidate examinations. The team implemented a backlog mitigation strategy that eliminated nearly 23,000 latent prints from the backlog in six months. Major successes included identifications of high-value targets including IED makers — one U.S. Special Operations Command (USSOCOM) enrollment in July 2011 resulted in the identification of 120 latent prints and 34 IED events traced to a single individual, now in custody. In September 2011, follow-up efforts from the BES team resulted in the identification of the suicide bomber who assassinated former Afghan President Burhanuddin Rabbani.

JAILBREAK

On April 25, 2011, more than 475 inmates, many of them Taliban insurgents, escaped through a tunnel from the Sarposa prison on the edge of Kandahar in southern Afghanistan. Within days, 75 of the men were recaptured at border crossings, routine traffic stops and even a recruiting station where one individual was already trying to infiltrate security forces. Many of the captures occurred with support from biometric data that the U.S. Central Command (USCENTCOM) requested from the BIMA — mostly fingerprint files and facial and iris scans from the prisoners' earlier enrollments.

MODERN ARCHITECTURE

In March 2011, the BIMA achieved a major milestone: Army approval of the 2010 As-Is Biometrics Enterprise Architecture (BioEA). This is the DoD biometric community's first delivered reference architecture. The As-Is BioEA establishes the strategic framework for delivering enduring biometrics capabilities to the DoD and its mission partners. In December 2010, the BIMA had achieved an earlier milestone with the delivery of the 2015 To-Be BioEA. The As-Is BioEA provides a baseline for moving from the 2010 environment to the 2015 To-Be environment, which will be a net-centric, service-oriented target state in which information and capabilities are securely available services on the network.

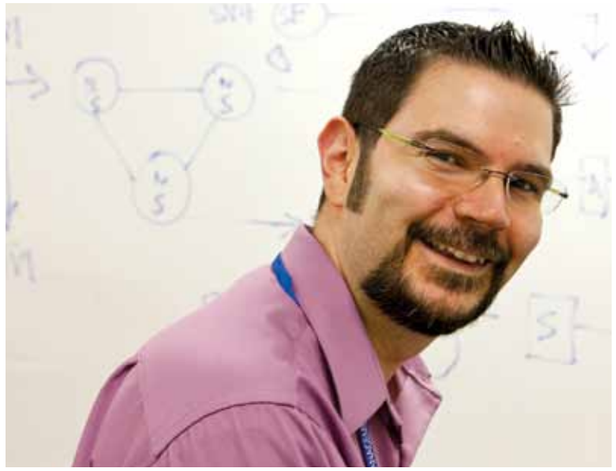
The BioEA has already had an impact providing insight into interoperability issues across programs, enabling developmental efforts like the Department of the Navy's Identity Dominance System to efficiently plan, design and develop interactions with the Biometrics Enterprise's authoritative database. What this means to the warfighter is that DoD personnel can use authoritatively matched biometrics data confidently, regardless of system solution. Collaborating across the COCOMs, Services and agencies, the BioEA has helped to ensure that biometrics are integrated into the planning and execution of missions and tasks across the full range of military operations and the DoD's business processes.

Throughout FY11, in accordance with DoD Directive 8320.02, and following DoD Guidance 8320.02-G, the BIMA continued to sponsor a Biometrics Data Sharing Community of Interest (BDS COI) on net-centric data sharing. The BDS COI includes partners from the DoD, other U.S. government agencies, industry and academia who meet several times a year to refine and verify the Biometrics Enterprise data architecture products: the Core Logical Data Model, the Integrated Data Dictionary, the Biometrics Glossary and the Biometrics Ontology.

WATCHING FOR BAD GUYS

Throughout FY11, the BIMA supported data standardization of the DoD Biometrically Enabled Watchlist (BEWL). This allows for a standardized method to produce mission-tailored watchlists that account for actions permitted under rules of engagement, status of forces agreements and

HIGHER STANDARDS



"We don't build the system or the data collection device. We build the vision."

GIOVANNI DEMONTE, BIMA

Chief, Architecture and Standards Branches
Arlington, Va.

DeMonte, a former U.S. Air Force Communication/Navigation specialist with a background in telecommunications, was running one branch, Architecture, when a staff reshuffling this year added the Standards branch to his plate. Wearing his Architecture hat, DeMonte thinks big picture, mapping out systems and processes from an eagle-eye view across the Biometrics Enterprise. "We don't build the system or the data collection device. We build the vision," he says. "We've identified what's already there in the As-Is Architecture, and look for ways to tie it all together more efficiently at the Enterprise level in the To-Be Architecture." Wearing his Standards hat, he ensures that the various collection devices and data formats are synchronized across the DoD for interoperability. His work in both branches informs his ongoing solution to a persistent question: "What additional services can we provide to the Enterprise with existing resources?" Similar to how smartphones keep offering new and diverse services without adding hardware, DeMonte sees an evolving target state for DoD Biometrics: "One system, many services."

the laws of armed conflict that vary by country and mission. In FY11, the BIMA also developed a new version of the DoD Electronic Biometric Transmission Specification (EBTS v3.0), which allows for additional capabilities to help identify persons of interest. The DoD and Intelligence Community Biometrics Focus Group continues to build consensus and generate change requests three times per year for the adoption of all biometrics-related standards used across the Enterprise into the authoritative standards repositories. The BIMA is a key participant in national and international standards bodies on biometrics and security techniques: International Committee for Information Technology Standards (INCITS) M1 (Biometrics 1) and INCITS CS1 (Cyber Security 1), JTC 1 (Joint Technical Committee 1)/SC37 (Subcommittee 37) and JTC 1/SC27. The team served as an editor and primary contributor for the development of International Organization for Standardization/ International Electrotechnical Commission (ISO/ IEC) 19794-1, Amendment 2, on Conformance Testing Methodology for Biometric Data Interchange Formats. This standard allows testing organizations to validate conformance of biometric data records to the applicable data format standards, and helps ensure interoperability of biometric data interchanges.

CONFORMITY

To ensure consistent adoption, development and implementation of biometric standards and methodologies, the BIMA actively led and participated in national and international Standards Development Organizations. BIMA personnel worked closely with the National Institute of Standards and Technology (NIST), which chairs the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management, Standards and Conformity Assessment Working Group (SCA WG). The BIMA actively participated in the SCA WG to ensure DoD coordination and alignment with federal partners on the development of policy for the adoption and implementation of biometric standards and standardized testing methodologies. The BIMA provided input to the following documents developed and maintained by this group: Registry of USG Recommended Biometric Standard; NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards; Catalog of Active Biometric Test and Certification Programs; and Biometric Interagency Test Evaluation Schema Technical Report.

The BIMA developed enhanced fingerprint and face biometric sample quality measurement algorithms and tools based on national and international biometric data format and quality standards. The BIMA is currently developing iris quality measurement algorithms and tools to increase the matching performance for iris images. The quality scores can be used to gain a level of confidence that high-quality images are submitted to recognition systems, and will ultimately increase interoperability.

The BIMA chaired the DoD Biometrics Standards Working Group (BSWG) to provide a forum for consensus building and technical considerations related to biometric standardization. On behalf of the Defense Information Systems Agency (DISA) and under the direction of the EM for

DoD Biometrics, the BIMA chaired the DoD and Intelligence Community Biometrics Focus Group. This group develops consensus across the Biometrics Enterprise acquisition stakeholder community, and biometric subject matter experts, to research and provide biometric and biometrically enabled intelligence standards recommendations to the Joint Enterprise Standards Committee (JESC). These standards can be adopted into the DoD Information Technology Standards Registry (DISR) and Intelligence Community Standards Registry (ICSR) authoritative databases. Finally, the BIMA participated in DoD/NATO standards collaboration, working on the development of the first ever NATO Biometrics Standardization Agreement (STANAG).

BIOMETRICS AND FORENSICS: A DOUBLE THREAT

In addition to serving as EA for DoD Biometrics, the Secretary of the Army is now also EA for DoD Forensics. FY11 saw increased collaboration between the BIMA and the Army's Office of the Provost Marshal General (OPMG), the Responsible Official (RO) for DoD Forensics. The BIMA also continued collaborative efforts with the Armed Forces DNA Identification Laboratory (AFDIL) to explore ways to better correlate biometric identities submitted to the DoD ABIS or AFDIL's Laboratory Information Systems Applications (LISA) database.

While DNA is well-suited for forensics, the DoD recognizes that there are considerable policy and technical challenges in applying DNA as a biometric tool. Unlike other modalities, DNA does not have a template and requires two samples to compare for matching. Also, DNA matching is not as automated as the matching of other modalities such as fingerprint, iris scan, palm print and facial recognition. The BIMA is keeping abreast of improvements in matching efficiency and reduction of sample size, particularly advances in rapid DNA and touch DNA.

Another successful trend in the BIMA's forensics work involved expansion outside the DoD to state and federal agencies as well as the private sector. In FY11, the BIMA developed a relationship with the International Association for Identification, the world's oldest and largest professional forensics organization. The BIMA presented an exhibit at the American Academy of Forensics Science Conference, and supported the development and completion of the ROTC Forensic and Biometric Intern Program held at the National Forensic Science Technical Center.

ENABLE THE MISSION

On land or at sea, on base or far outside the wire, DoD Biometrics powered by the BIMA take identity and put it to work for informed decision making. For the Soldier hunting terrorists in Kandahar Province, the border official on the U.S.-Mexico border, the Navy SEAL boarding an unfamiliar vessel or a Marine providing disaster relief in stricken countries, biometrics help bring transparency to an opaque situation.

SUPPORTING THE WARFIGHTER

Supporting the warfighter remains a central part of the BIMA's mission. In FY11, the

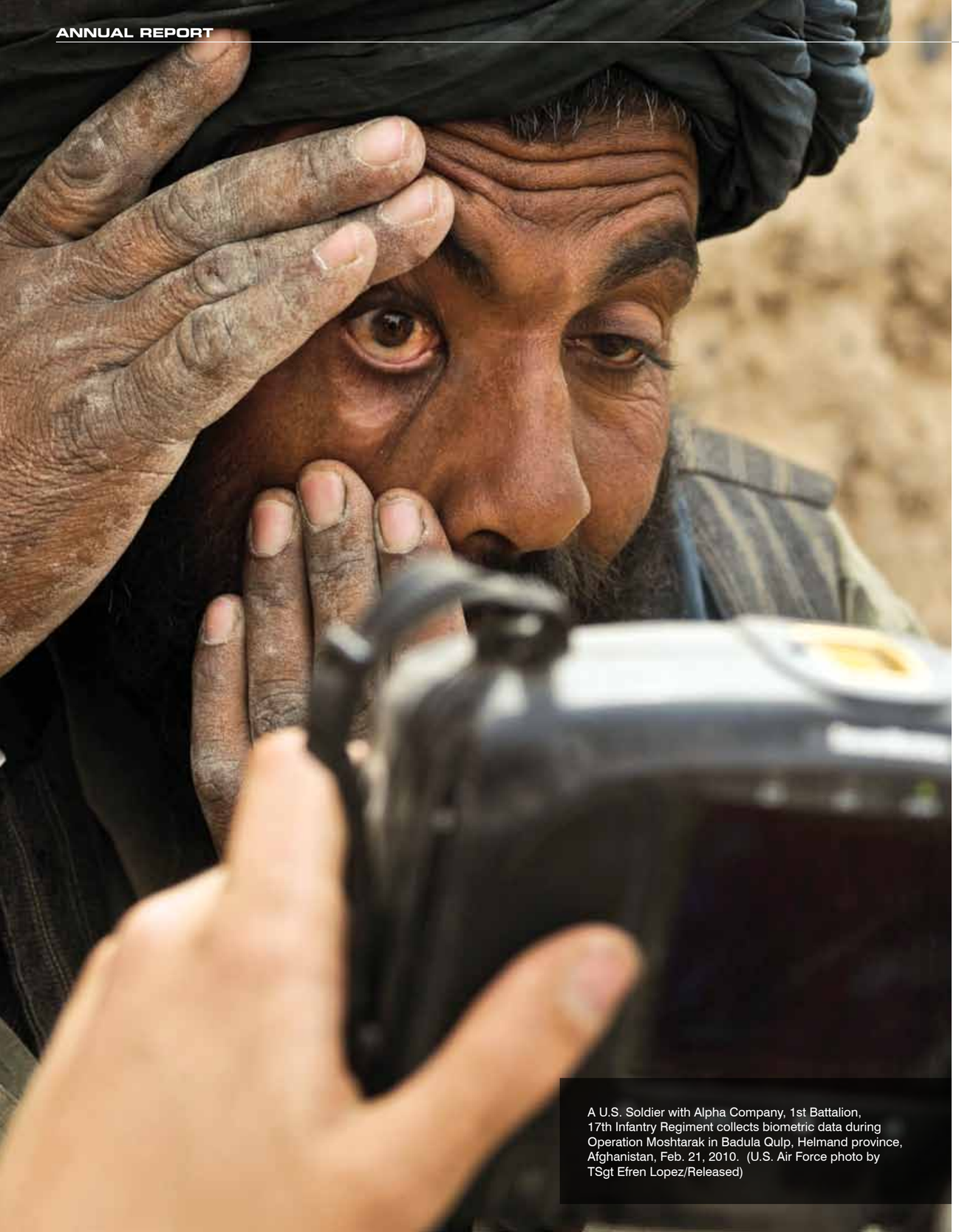
THE ONE-TWO PUNCH

VON GRETCHEN BEARD-MITCHELL, BIMA

Physical Scientist (Future Modalities)
Arlington, Va.

"Without collaboration among partners such as DoD, the Department of Homeland Security and the international forensics community, biometrics cannot produce their fullest benefits," says Beard-Mitchell, a former U.S. Army officer and the agency's resident expert on forensics. "Biometrics," she says, "offer a verification application such as physical and logical access control, whereas forensics are most often associated with gathering and analyzing physical evidence from crime scenes to identify criminals and their victims. Biometrics and forensics can operate together to analyze human traits at a crime scene or during surveillance to gather a positive identification," she adds. "My biggest concern is how the biometrics community may not understand just how much biometrics and forensics overlap and support each other. Not only does the safety of my husband, who's currently deployed in Afghanistan, keep me up at night, but so does knowing that Soldiers and leaders lack the knowledge of how the forensics and biometrics fields would aid in the safety and mission of the officers, as well as the men and women serving under them."

> "Biometrics and forensics can operate together to analyze human traits at a crime scene or during surveillance to gather a positive identification."



A U.S. Soldier with Alpha Company, 1st Battalion, 17th Infantry Regiment collects biometric data during Operation Moshtarak in Badula Qulp, Helmand province, Afghanistan, Feb. 21, 2010. (U.S. Air Force photo by TSgt Efren Lopez/Released)

BIMA participated in the completion of the *Commander's Guide to Biometrics in Afghanistan*, published by the Center for Army Lessons Learned, an effort that involved cross-agency coordination at multiple levels of command. This handbook serves as the most advanced and detailed biometrics guide for battlefield doctrine, enabling current commanders to operationalize biometrics. The first print run produced 6,000 copies, which were distributed with the U.S. Army Training and Doctrine Command (TRADOC) Capability Manager's video graphic on biometrics and the Military Decision Making Process.

In FY11, the BIMA began an update of the *DoD Capstone Concept of Operations (CONOPS) for Employing Biometrics in Full-Spectrum Military Operations*, which is ongoing. The BIMA also supported OSD in starting the review and revision of the DoD Directive for Biometrics 8521.01E, soliciting input from internal and external stakeholders in preparation for formal staffing expected by the end of the year. The BIMA enabled a quick-training capability for Army units as a result of the updated series of existing Handheld Interagency Identity Detection Equipment (HIIDE) Graphic Training Aids, which forms the groundwork for leveraging the system to promulgate biometric capabilities at the tactical level.

The BIMA also assisted in drafting an Operational Needs Statement (ONS) as the baseline requirement for biometric equipment to be used in home station training by the U.S. Army Forces Command (FORSCOM) and First Army. The ONS has been validated, and as a result PM DoD Biometrics is now providing equipment to fulfill these requirements. The equipment will enable Army units to carry out their mission with more flexibility by providing enhanced biometrics home station training to Soldiers rather than depending on Mobile Training Teams or Combat Training Centers.

> "The birthdays and the names are rarely the same, but the biometrics never lie."
>
> Don Walker
> DoD ABIS Watch Desk Manager
> Clarksburg, W.Va.

The BIMA made its training webpage more accessible to a wider variety of U.S. personnel by allowing Service members to access biometrics training material on both the Joint Knowledge Information Fusion Exchange (JKnIFE) and the Defense Knowledge Online (DKO) portals.

Finally, the BIMA assisted USCENTCOM and FORSCOM in updating biometrics predeployment training requirements with the latest Techniques, Tactics and Procedures derived from lessons learned in Iraq and Afghanistan.

QUICK HITS

On Nov. 16, 2010, USSOCOM Forces detained and biometrically enrolled two suspects during a raid on an objective in Afghanistan. A month later, on Dec. 25, USSOCOM again detained and enrolled the men for suspected terrorist activities during a raid on a different objective in the region. Their enrollments were submitted to the DoD ABIS and resulted in a hit to their November enrollments. The status of the two suspects was Tier 4 (Do Not Hire; Deny Base Access; Disqualify for Police or Army Training).

TECHNOLOGY: LEANING FORWARD

The BIMA's technology focus in FY11 transitioned away from current concepts and technologies that could be leveraged in support of today's warfighter requirements. Instead, the BIMA is focusing on longer-term capability gaps and the development of strategies to meet tomorrow's challenges. Several key initiatives demonstrated by the BIMA at Marine Corps Base Quantico, in Virginia, in the prior fiscal year became in-theater pilots in FY11. Examples include a Web services watchlist template server, finger quality graphing tool and case management Web services. The BIMA hosted experimentation events and participated in work in Arizona at Fort Huachuca and Yuma Proving Ground. That work has culminated in final preparations for in-theater pilots. The BIMA continued to collaborate with the U.S. Army Science Board and its work on non-cooperative biometrics, as well as the Service labs, academia and, indirectly, with industry.

INTEROPERABILITY

The BIMA shares DoD biometric data with partners including operational military forces, the intelligence community, the personnel security community and interagency partners such as the FBI, DHS and the Department of State (DOS). Interoperability also extends to international partners; Memorandums of Cooperation (MOCs) were signed with Afghanistan in January 2011 and Germany in July 2011, setting the conditions for the sharing of biometric data with the DoD ABIS. The information provided by the BIMA enables and supports security missions such as the targeting of high-value individuals, maritime interdiction operations, physical and logical access control, disaster relief, humanitarian assistance, security operations, in-theater interagency operations, access to services for non-U.S. persons, border protection and more.

THE BIOMETRICS TRIAD

Biometrics offer critical applications from the battlefield to the borders of the homeland. Therefore, the BIMA has a special data-sharing relationship with two key partners: DOJ — particularly the FBI Criminal Justice Information Services (CJIS) Division—and DHS. The DoD ABIS already conducts fully automated data sharing with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) database. Throughout FY11, the BIMA made strong advances toward the same level of interoperability with DHS' automated biometric identification system (IDENT) database. Interoperability between the DoD ABIS and IDENT represents the last remaining portion of

IDENTITY DOMINATORS

COL NATALIE JACARUSO, U.S. ARMY, BIMA
Military Deputy
Arlington, Va.

COL DOUGLAS FLOHR, U.S. ARMY, BIMA
Deputy Director, Operations
Clarksburg, W.Va.

Knowledge may be power. But for the U.S. military, it's also a weapon system.

On today's asymmetric battlefields, American Soldiers and Marines routinely use biometrics to know with certitude whom they're up against. That knowledge allows our forces to better manage chaotic battlespaces, and make critical decisions with more assurance and confidence. It's been an evolving process. "Sometime between '06 and '07 in Iraq, that's when biometrics became a game changer," says Jacaruso, an Iraq veteran who had a key role in establishing biometrics within Operation Iraqi Freedom. "Biometrics went from a bunch of devices and this space-age technology to an operational weapon system, which changed the way we fight. It allowed us to develop identity dominance." That concept refers to a commander's ability to fully dominate his or her area of responsibility by knowing the true identities of those within it. "The importance of biometrics is the ability to identify friend from foe at the tip of the spear," notes Flohr, also an Iraq veteran. "A lot of our enemies are not wearing uniforms anymore. You have to be able to identify them. Biometrics give you the tools to do that. Biometrics are facts. You can attempt to hide on the battlefield. You can attempt to lie to an American Soldier. Biometrics won't let you do that."

> "The importance of biometrics is the ability to identify friend from foe at the tip of the spear."

the Biometrics Triad, per Homeland Security Presidential Directive (HSPD) 24's mandate for interagency biometric data sharing. The DoD ABIS already shares high-priority biometric datasets with key customers at DHS, such as Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP) and the U.S. Coast Guard (USCG). These organizations utilize the DoD architecture to submit directly to the DoD ABIS, which facilitates the automated passage of the data to DOJ and then to DHS.

The path to full and automated interoperability involves solving not just technical challenges but policy issues. The BIMA contributed to the resolution of both challenges this year by supporting an OSD-led effort that resulted in the signing of a Memorandum of Agreement (MOA) between the DoD and DHS on March 23, 2011. The MOA governs interoperability and leads to automated processes for sharing data. Through its lead role on the Integrated Project Team (IPT), co-chaired by DoD and DHS officials, the BIMA validated DoD stakeholder requirements for interoperability through a Joint Functional Requirements Document. The BIMA continues to analyze and implement interim solutions to interoperability through the use of the FBI's IAFIS. Interoperability between the DoD ABIS and IDENT will better enable DoD ABIS customers to identify adversaries and protect personnel and infrastructure overseas and at home. The signing of the MOA in March provides the policy foundation for the IPT to move forward to full interoperability between the DoD and DHS, projected to occur in fall 2012.

LOOKING SOUTH

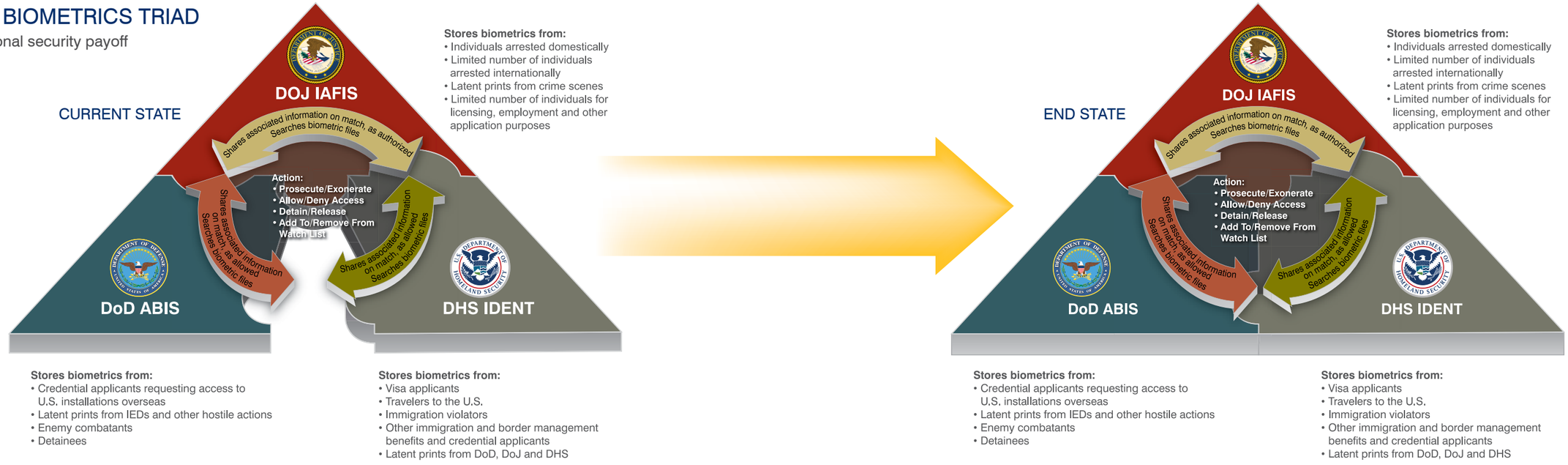
In February 2010, intelligence analysts with the U.S. Special Operations Command South (USSOCSOUTH) deployed to the U.S. Embassy in Quito, Ecuador, to support the ICE Attaché Office during investigations of Ecuador-based Middle Eastern and African networks engaging in illicit trafficking of humans, weapons, cash and narcotics. During a two-week deployment, 19 individuals were biometrically enrolled at Quito's Mariscal Sucre International Airport. The following June, when two individuals were detained by CBP officers in the desert near Tucson, Ariz., both were fingerprinted. One provided a hit to one of the February Quito enrollments, despite the fact that he had traveled through Ecuador under a different name and with different travel documents than when he was detained in Arizona. His travel companion claimed loose ties to Harkat ul-Jihad al-Islami Bangladesh, a terrorist organization, and both were denied asylum to the U.S. As a result, ICE increased its investment in biometrics throughout the U.S. Southern Command (USSOUTHCOM) Area of Responsibility (AOR). Additionally, Ecuador's government implemented visa requirements for citizens of nine Middle Eastern and African countries.

COCOM ENGAGEMENT

Biometrics powered by the BIMA have facilitated the building and strengthening of key relationships with our interagency partners and foreign governments to confront challenges such as international drug trafficking, special

THE BIOMETRICS TRIAD

A national security payoff



interest aliens and other potential adversaries. For example, biometrics have served as a door-opener for USSOCSOUTH and USSOUTHCOM to work more closely with ICE, the Drug Enforcement Administration (DEA), the FBI and foreign governments.

Beginning in fall 2010, the BIMA's operational activities supported the U.S. Africa Command's (USAFRICOM's) Noncombatant Evacuation Operations (NEO) to integrate biometrics into the NEO Tracking System, mission analysis and Horn of Africa AOR for maritime and border security. The BIMA remains engaged with USAFRICOM on current initiatives such as fusing biometrics, forensics, and exploitation of media and documents; trying to get manpower and equipment to the Service components through USAFRICOM resources; installing base-access systems; establishing a USAFRICOM portal for biometrics submissions; conducting security vetting on partner nations involved in training and exercises; and providing equipment to those nations for maritime and border security.

The BIMA funded Identity Operations Managers (IOMs) in the COCOMs in FY11 with an implied mission to establish enduring biometrics capabilities in support of the DoD Biometrics Enterprise. IOMs coordinate with the BIMA for the synchronization and integration of identity management capabilities, and support the development of the appropriate COCOMs' Biometrics CONOPS for their mission sets. The BIMA conducts quarterly program management reviews on the use of IOM resources and contributions.

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 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 Internment 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 the DoD with DHS.

BITMAP

The Biometric Identification Transnational Migration Alert Program (BITMAP), begun in fall 2010, moved worldwide and marked a solid achievement for the BIMA in FY11. The program, run jointly by ICE and the DoD, enables the two organizations to submit data cooperatively to the DoD ABIS, with throughput to the FBI's IAFIS and DHS' IDENT, resulting in efficient responses to ICE agents, Soldiers, Sailors and Marines on the ground. These agents saw matches on individuals enrolled previously in the USCENTCOM AOR. The program has also enabled the collection of hundreds of thousands of "hard cards" from the criminal files of various foreign countries, complete with fingerprint data, which will be migrated to the DoD ABIS once throughput challenges of such a large dataset are handled. The payoff to the BIMA's customers is understanding what resources are available to transfer biometrics

THE STRENGTH IN SHARING

STEPHANIE DEMARCO, DEPARTMENT OF HOMELAND SECURITY, US-VISIT

Project Manager, DHS/DoD
Interoperability Project
Arlington, Va.

The field of biometrics creates careers.

When DeMarco entered college more than a decade ago and began earning her degree in management information systems, DHS and the BIMA didn't exist. Today, with a master's degree in project management, she spent most of FY11 as the DHS point person at U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT), collaborating with the BIMA to bring DoD's ABIS and DHS' IDENT databases to full interoperability, projected for late 2012. Interoperability between federal agencies is crucial. "It's a very complex initiative," she says. "In the beginning, I had to learn BIMA's organizational structure. Now, I can look back and say that it's been a pleasure working with everyone and watching the relationship between agencies grow." Most of all, DeMarco says she's pleased to contribute to our national security by implementing the tenprint biometric capture devices at DHS ports of entry that have allowed for increased data-sharing between agencies. "DoD shares important data to assist DHS in immigration enforcement and providing immigration benefits. Sharing this data with the Department of State also enables DHS to keep out those individuals who should not be in the U.S. Interoperability between agencies has strengthened the security of our nation."

> "Interoperability between agencies has strengthened the security of our nation."

> "You can't change biometrics. They are yours. There is no forging it, no faking it."
>
> CAPT James Fossa, U.S. Navy
> Director of Biometrics in Iraq
> — *Army Times*, Aug. 29, 2011

information, and receiving operational help from BIMA staff who can identify the current capabilities of the systems and help customers develop requirements for identity solutions.

REQUIREMENTS MANAGEMENT

Throughout FY11, the BIMA dealt on a daily basis with the J-8, the Army G-38 and G-3/5/7, and primarily the Department of the Army Military Operations – Capability Integration Division (DAMO-CI). A BIMA liaison officer to the J-8 enhanced the agency's relationship with the J-8 throughout the year. This gave the BIMA better visibility across the Enterprise, and helped the BIMA better coordinate processes and capabilities within the Enterprise. The BIMA completed populating its requirements management repository into the Dynamic Object-Oriented Requirements System (DOORS). This tool facilitates requirements traceability across the Enterprise. The uploading of source documents such as the Capabilities Development Document, Capabilities Product Document, System Requirements Specifications and Architectural Views provide the required details for determining operational, system and technical needs toward the delivery of biometrics capabilities. Examples of these documents include the Biometrics Enabling Capability (BEC), the Next-Generation DoD ABIS (NGA) and eventually will include additional Joint Capabilities Integration and Development System (JCIDS) documents and system specifications. BIMA staff also provided Enterprise-level perspective on the Joint Urgent Operational Needs Statement (JUONS) for Data Synchronization and Improved Tactical Handheld. The BIMA hosted and completed the BEWL Tiger Team as directed by the Joint Biometrics Operational Coordination Board (JBOCB), providing information to support design resolution for the Navy's Information Dominance System. The BIMA provided significant input, oversight and support in FY11 to the development of these Capabilities Development Documents, which ensures that the DoD will be able to establish two programs of record for biometrics: The BEC and the Joint Personnel Identification (version 2). The approval and validation by the DoD of the documents allows the acquisition community to further develop new authoritative repository and joint collection/capture devices for biometrics.

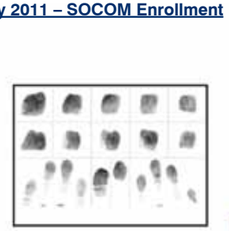
THE SUPER HIT

On July 21, 2011, at 6:45 p.m., while many Americans on the East Coast might have been gathered around the dinner table, BIMA staffers in Clarksburg, W.Va., were hard at work monitoring their computer displays. Suddenly, an enrollment arrived from the U.S.

THE SUPER HIT

21 July 2011 – SOCOM Enrollment

Name: XXX
DOB: XXX
HT: 5' 06"
WT: 133
Eyes: BROWN
Hair: BLACK



- **120 IED Related Latents**
- **34 Distinct IED Cases Links**
- **Two (2) DoD Enrollments**
- **Two (2) Interagency Enrollments**
- **One (1) DoD Detainee Enrollment**

Background

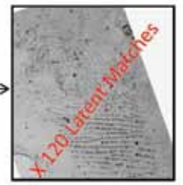
March 2011: IED related evidence was received and processed by multiple agencies between May 2010 and July 2011. The latent prints were submitted with no significant identifications and added to the DoD ABIS Unsolved Latent File.

Unsolved Latent Files

DoD Enrollment

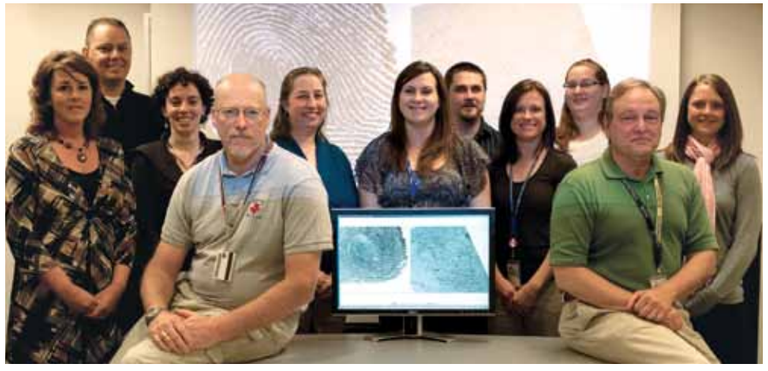
Latent Case: ######
Priority Code: Green

IED Related Latent



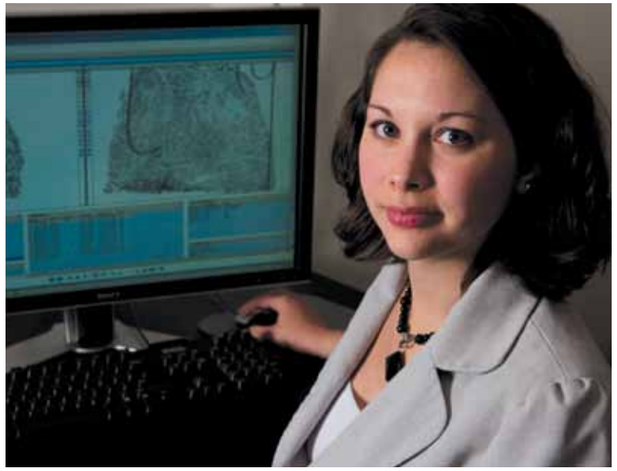
Latent Case Print

21 July 2011: The subject was encountered and enrolled by DoD elements due to suspicion of terrorist activities resulting in multiple unsolved latent matches confirmed by BIMA's Biometric Examination Services Team.



Watch Desk staffers and Fingerprint Examiners from the BIMA's Clarksburg facility pose with prints from their biggest catch of FY11.

MYSTERY SOLVERS



> "All the computers beep. We know a high priority is waiting, and it's a matter of who grabs it first."

ALLISON MILLER, BIMA

Biometric Examination Services Team
Clarksburg, W.Va.

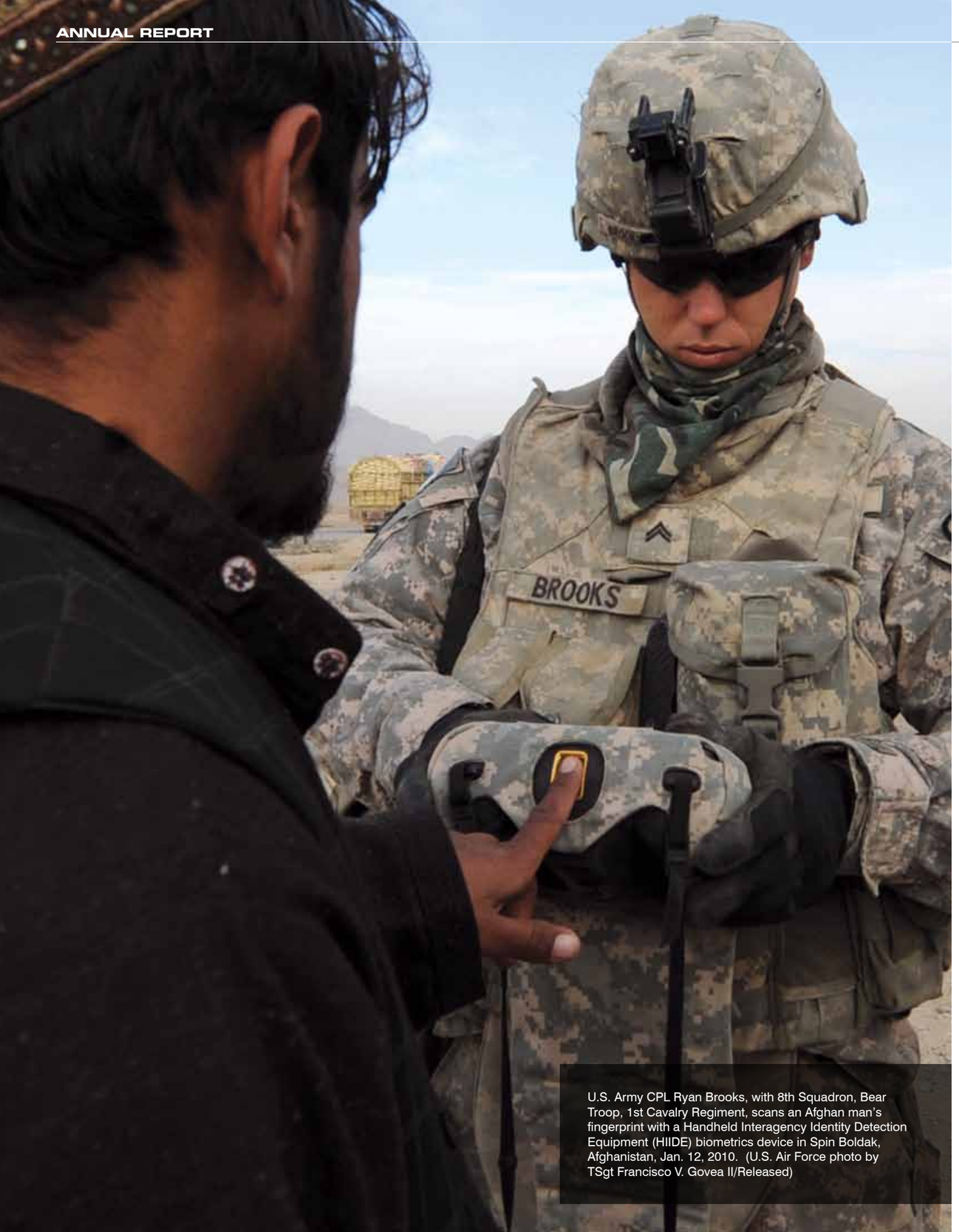
She knows fingerprints like the back of her hand. Miller, a Certified Latent Print Examiner (CLPE), will compare hundreds of fingerprints most days — and thousands other days. "They're unique, and they're permanent," she says. The friction ridges on human fingers, toes, palms and feet begin to form in the 10th week of gestation, and are fully formed by the 17th week. "Sixty-five percent of human fingerprints are loops; 30 percent are whorls; and 5 percent are arches," she says. "That frequency has remained over many, many years. It's a mystery." Miller deals in solvable mysteries for the DoD, such as helping to determine who's making and detonating Improvised Explosive Devices (IEDs) in Iraq and Afghanistan. She compares prints of detainees to latent, or unknown, prints that have been searched by Biometric Examination Services (BES) team members in the DoD Automated Biometric Identification System (DoD ABIS), many of them taken from the fragments of IED events. When a new, high-priority enrollment comes in and there is a potential latent match, the quiet room she shares with other examiners, packed with high-resolution flat screens, gets busier. "All the computers beep," she says. "We know a high priority is waiting, and it's a matter of who grabs it first."

Special Operations Command (USSOCOM). In minutes, latent print examiners determined that the fingerprints of the new individual matched latent prints already collected from multiple Improvised Explosive Device (IED) events — the eventual count reached 34 events with 120 latent prints — stored in the DoD ABIS' Unsolved Latent File. Between May 2010 and July 2011, the DoD ABIS had received multiple cases containing the latent prints of one individual whose ridge flow displayed a distinctive whorl. "We knew of some of the linkages because at the time we were doing latent-to-latent comparisons," says Certified Latent Print Examiner Lindsay McAvoy. "However, when those prints were submitted, ABIS did not contain a tenprint record of the individual in question." It wasn't until July 21, 2011, that the first tenprint record of him was submitted into the DoD ABIS. "The examiners working the unsolved latent match recognized his prints immediately," she says. The Biometric Examination Services team responded promptly to USSOCOM Forces, who detained the individual. This Super Hit, which marks a record number of IED events traced to one individual, demonstrates the BIMA's continuing ability to connect the dots in pursuit of the most elusive and dangerous adversaries. "It's nice to have a job where you work diligently and see the rewards," says the BIMA's Enterprise Operations Division Chief Cheley Gabriel. "Our people are proud of what they do on a daily basis. Everyone in my division understands that they are part of a team."

COLLABORATION WITH ACADEMIA

BIMA research and development funding moves through approved military channels such as the U.S. Army Armament Research, Development and Engineering Center (ARDEC) in Picatinny, N.J., and arrives at private institutions of higher learning including West Virginia University, Clarkson University and Carnegie Mellon University. Researchers at Carnegie Mellon's CyLab are developing algorithms for robust face and iris biometrics and pattern recognition, long-range iris acquisition and identification, and the generation of 3D face models from single 2D images. The BIMA keeps abreast of cutting-edge research at these institutions through Biometrics Technology Demonstrations (BTDs) that may one day become operational applications to supplement the agency's current portfolio of modalities.

The BIMA is also a member of the Center for Identification Technology Research (CITeR), a National Science Foundation Industry/University Cooperative Research Center comprised of government agencies such as the FBI and DHS, labs such as NIST and major defense contractors. CITeR advances the performance of biometric and human credibility assessment systems through the cross-discipline research of enabling technologies, interdisciplinary training of scientists and engineers, and facilitation of new technology transfers to the private and government sectors. The BIMA holds two memberships with CITeR to more fully advance its research needs and better reap the benefits of academic expertise.



U.S. Army CPL Ryan Brooks, with 8th Squadron, Bear Troop, 1st Cavalry Regiment, scans an Afghan man's fingerprint with a Handheld Interagency Identity Detection Equipment (HIIDE) biometrics device in Spin Boldak, Afghanistan, Jan. 12, 2010. (U.S. Air Force photo by TSgt Francisco V. Govea II/Released)

PROTECT INFORMATION, IDENTITIES, PEOPLE

To identify and enable leads to the ultimate payoff of biometrics: protection. This is reiterated in the BIMA's vision statement: "Protect the nation through the employment of biometrics capabilities." From a practical standpoint, it's about protecting people, installations and classified information at home and abroad. Conceptually, it's about protecting the advantage, the mission and the shared ideals of freedom and democracy. Protection is the true measure of the success or failure of the Biometrics Enterprise.

MEASURING SUCCESS

The BIMA performed 62 separate events for standards conformance, interoperability and supportability testing of biometrics-enabled programs and systems in FY11. Test engineers planned, executed, analyzed and reported on 13 separate evaluations in support of USSOCOM, USCENTCOM, USSOUTHCOM, Army G-2 and other DoD and U.S. government sponsors. The agency maintains and updates its Conformance Products List (CPL), which provides leaders and decision makers across the Biometrics Enterprise with a listing of biometrics-enabled technologies and vendors who have been assessed and meet CPL criteria. Additions, deletions and modifications to the CPL, which currently has 51 products, occur continually. Furthermore, the BIMA completed duties and responsibilities as the Participating Test Unit Coordinator (PTUC) for the Biometrics Community of Interest in accordance with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E. These responsibilities provide the customer or stakeholder with guiding principles, test procedures, standards conformance, functionality and DoD ABIS integration test data for the best deployment decisions. Laboratory and operationally realistic environment tests included the Multilingual Automated Response System (MARS), which uses the Secure Electronic Enrollment Kit (SEEK) I and II hardware, the HIIDE, the Mission Oriented Biometric Software (MOBS) and the Cogent Fusion Multimodal Biometric Handheld Device.

The BIMA coordinated and initiated an HSPD 12 pilot with the U.S. Army Accessions Command (USAAC) to perform background investigations on potential Army recruits. In early FY11, the BIMA achieved accreditation to the National Voluntary Laboratory Accreditation Program (NVLAP) from NIST for services listed on the Scope of Accreditation NVLAP Lab Code 200933-0, for Biometrics Testing. The BIMA was the first biometrics testing laboratory to receive this, which demonstrates technical competence for a defined scope and operation of laboratory quality and management systems. It also provides credibility to the quality and management processes BIMA test engineers use to conduct test events, experiments and internal and external audits; and collect, track, analyze and report operational performance metrics for the biometrics community.

PRIVACY

In FY11, the BIMA initiated a thorough review of its privacy program to validate and strengthen

> "The warfighter believes in the power of biometrics exploitation and identity operations. Units like SOCOM search the DoD Biometric Authoritative Database, even on Christmas Day. This capability is relied upon by our command 24/7/365."
>
> Craig J. Archer, Identity Superiority Manager, USSOCOM

policies and processes for protecting information throughout the biometrics life cycle, from collection and storage to use and disposition. This proactive approach will sustain privacy as a top priority, while allowing DoD Biometrics users to exploit information in support of DoD military operations and business functions. Utilizing technological advancements and best practices in information security, the BIMA addresses potential pitfalls and guarantees the secure use of biometrics for mission success.

DOD IDENTITY ASSURANCE

Since April 2010, the Identity and Privilege Management Working Group has been charged by the Identity Protection and Management Senior Coordinating Group (IPMSCG) to lead DoD efforts on creating a roadmap and implementation guidance for the DoD's Identity Management Strategic Plan. The BIMA has actively participated in the group, even providing an embedded action officer to the Office of the DoD Chief Information Officer, who is leading the effort. During FY11, the group and the products evolved to emphasize a new overarching term: Identity Assurance (IdA).

IdA is a comprehensive DoD framework to mitigate the rapidly increasing national security risk of adversaries utilizing fraudulent identities and credentials to achieve unauthorized access to U.S. property, networks and information. IdA balances protecting privacy with maximizing the ability to deny anonymity to transnational threats. It does this by sharing identity information with domestic and international partners to support near-real time, global identity authentication. Effective DoD-wide governance is required to unify policies, processes, standards and enterprise capabilities that bind the physical and digital representations of entities — and enable the integrity, privacy, authenticity and availability of identity information across all DoD mission environments. Accomplishing the following strategic goals will establish an IdA capability/framework for the department:

- Unity of purpose for effective governance and employment: Unified governance ensures that a focused strategy is employed to mitigate risk, limit redundancy, bridge stovepipes, and enable secure information-sharing and coordination with domestic and international mission partners.
- Institutionalize an IdA culture across the department: This provides a common understanding of identity issues across all mission environments through the development of a CONOPS, policies, processes, standards and terms of reference.
- Support transparent identity data-sharing activities between interagency, international and commercial mission partners: This effortless capability allows mission owners to share identity information across all military, governmental and commercial networks that will enable effective transactions in the global cyberspace.
- Enable the development, deployment, operation and maintenance of a reliable, interoperable and secure department-wide capability: Alignment of strategic, operational and technical materiel investments across all mission environments ensures identity and information assurance in support of access management.

The events leading up to 9/11 illustrate the importance of sharing identity information with domestic and international mission partners, in order to establish global situational awareness of the true identities of persons and other entities of interest. This is a required capability for denying unauthorized access to U.S. property, networks and information. The IdA Working Group is developing a CONOPS and department-wide Implementation Guidance & Roadmap that positions the department to mitigate the risk of asymmetric and cyber threats. These threats use fraudulent identities and credentials to exploit the intrinsic vulnerabilities in open societies that value civil liberties and personal privacy. Biometrics play a key role in IdA, which enables high confidence that an individual is who he or she claims to be. Furthermore, biometrics can enable personnel suitability screening by providing an additional means to check against authoritative and/or derogatory databases beyond traditional name-based methods.

THE TURBAN BOMBER

On Sept. 20, 2011, former Afghan President Burhanuddin Rabbani was holding peace talks in his Kabul home when a suicide bomber concealing an explosive in his turban entered the home unsearched and detonated the device, killing Rabbani and four of his bodyguards. A tenprint file on the bomber was submitted to the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and was automatically searched against the DoD Automated Biometric Identification System (DoD ABIS) with no matches. BIMA personnel in Clarksburg, W.Va., were suspicious of the failed match and obtained the file from the DoD ABIS Watch Desk for further analysis by the Biometric Examination Services (BES) team. Certified print examiners on the team noticed that the prints appeared to be out of sequence and corrected the errors. After resubmitting the file, the prints resulted in a hit to a person twice enrolled into the DoD ABIS in late 2009 — the turban bomber. One of the two files matched had been provided by a Coalition partner, underscoring the crucial role of international data sharing.

U.S. Marine Corps LCpl Maxx A. Juusola, with Charlie Company, 1st Battalion, 3rd Marine Regiment, cleans the finger of an Afghan man before using a Biometric Automated Toolset (BAT) device to record information about him in Marjah, Afghanistan, Feb. 22, 2010. Marines use the BAT to create a record of people living in an area. (U.S. Marine Corps photo by Cpl Albert F. Hunt/Released)

WAY AHEAD

The BIMA will continue to lead DoD activities in the coming months to program, integrate and synchronize biometrics technologies and capabilities. The methodologies and applications for biometrics will only expand with the needs and creativity of those who contribute data in-theater and those who receive and manage the data in the U.S. Biometrics, as an enabling tool to the warfighter, to business functions and to national security, have already become an irreplaceable national asset.

THE DOD ABIS

As the center of gravity for the many identity functions within the Biometrics Enterprise, the DoD ABIS will continue to grow in importance. The operation, maintenance and enhancement of the system are paramount to ensuring that the nation can identify threats and adversaries going forward. The DoD ABIS will continue to grow to handle the interagency and international data-sharing demands of our partners and allies.

EA AND EM

By facilitating long-term investment and consistently enhancing biometrics functionality, the Secretary of the Army will continue to fulfill the role as the EA for DoD Biometrics to institutionalize the capability as a core competency of the department. The Director, BIMA, as the EM for DoD Biometrics, will continue to lead DoD activities to program and synchronize biometrics capabilities; the Director will also continue to oversee the operation of the DoD authoritative biometrics database. This is important to the entire department and to the protection of the homeland, because biometrics are an increasingly vital key to security efforts in the fight against terrorism and to national security. The ability to establish an individual's identity with certitude and link the individual to past aliases or activities gives our military personnel a decisive edge, and aids other U.S. government organizations in their national security missions.

INTEROPERABILITY

Recognizing the critical nature of information sharing, the BIMA will continue to foster collaboration with a variety of partners to deny anonymity to the enemies of the U.S. and its allies. Interoperability of the DoD ABIS with operational military forces, the intelligence community, intergovernmental agencies and foreign partners continues to increase. Right now, the BIMA is putting the final technology and policy pieces in place to achieve interoperability with DHS in late 2012, streamlining and automating the sharing of biometric, biographic and contextual information. This will complete the Biometrics Triad of DoD, DOJ and DHS. Interoperability enriches the biometrics database used by border management and intelligence agencies, as well as federal, state and local law enforcement agencies, and increases the probability of identifying persons of interest across the U.S. government's many lanes of vigilance.

FORWARD-LOOKING ARCHITECTURE

The BIMA maintains a steady dialogue with COCOM, Service and Coalition partners as the organization moves from the As-Is Architecture, approved in March 2011, toward the To-Be Architecture of 2015. The To-Be BioEA will

HIGH SEAS SUCCESS

> "With two-thirds of the world covered by water, there's a good chance targets will try and go somewhere by boat."

LCDR KEN WASSON, U.S. NAVY

Maritime Security/Mine Warfare Officer
Naval Station Norfolk, Va.

"The Navy has taken an interest in biometrics for the same reasons it's important to everybody else," says Wasson, who trains and evaluates the Navy's elite Visit, Board, Search and Seizure (VBSS) teams based on the East Coast to carry out maritime interception and counter-piracy operations. "There are persons of interest out there trying to go different places. With two-thirds of the world covered by water, there's a good chance targets will try and go somewhere by boat." Biometrics, he says, empower VBSS operations "because we're boarding these vessels for a reason. We have intelligence that they're smuggling something, or that they're carrying somebody of interest." He's grateful for the quick turnaround on identifications. "If we had just that collection capability only, and we find out three days later that we had somebody, the ship could already be in port. Then we'd have to track it down, and three days gives somebody a big head start. But if we can get it sent off to the BIMA and get back a positive identification while we still have those people in our possession, while we're still on board the ship, then we can do something about it."

enable management of a portfolio of services spanning business processes, enterprise support and infrastructure, and utilizing techniques like gap-fit analysis to reduce duplication, all of which will contribute to the blueprint for future interoperability. Additionally, the To-Be BioEA will incorporate existing architectures and reference models such as the DoD Service Reference Model and the Net-Centric Enterprise Services program in order to leverage available Joint and federal capabilities to satisfy mission needs to avoid duplicating capabilities.

PRIVACY: A HIGH PRIORITY

The core capabilities of biometrics are uniquely and inextricably linked to individual privacy. As the agency responsible for the DoD's authoritative biometrics repository, the BIMA complies with federal laws and regulations to prevent unwarranted invasions of privacy. By continually assessing its privacy posture, the BIMA will work diligently in FY12 to gain the public's trust and confidence. The BIMA strives for transparency, allowing the public to know up front how their biometrics will be used. To further comply with privacy mandates and fair information practices, the BIMA has initiated an agency-wide review of the practical and desired uses of biometrics. This will enable DoD users to reinforce transparency and stay ahead of evolving mission requirements.

CONCLUSION

ENDURING CAPABILITY AND PROGRAM OF RECORD

The demand curve and operational appetite for biometrics will increase even with the drawdowns in Iraq and Afghanistan. It is essential that biometrics capabilities endure, and support current and future needs. Both the Army and the DoD recognize the value of biometrics — to the warfighter in the field, and to support national security and homeland defense. As a result, the DoD will need to retain, sustain and expand its biometrics capabilities, maintaining a global presence through activities such as direct action, training of partner forces, humanitarian missions and improving business functions. Over the last decade, DoD Biometrics has undergone a steady transformation from what was once a quick-reaction program to one now maturing into an enduring capability and program of record. Biometrics are here to stay.

ACRONYMS

ABIS	Automated Biometric Identification System
AFDIL	Armed Forces DNA Identification Laboratory
AOR	Area of Responsibility
ARDEC	U.S. Army Armament Research, Development and Engineering Center
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics and Technology
ASD(R&E)	Assistant Secretary of Defense for Research and Engineering
BAT	Biometric Automated Toolset
BDS COI	Biometric Data Sharing Community of Interest
BE	Biometric Examiner
BEC	Biometrics Enabling Capability
BES	Biometric Examination Services
BESP	Biometrics Enterprise Strategic Plan
BEWL	Biometrically Enabled Watchlist
BIMA	Biometrics Identity Management Agency
BioEA	Biometrics Enterprise Architecture
BITMAP	Biometric Identification Transnational Migration Alert Program
BSWG	Biometrics Standards Working Group
BTD	Biometrics Technology Demonstration
CBP	Customs and Border Protection
CITeR	Center for Identification Technology Research
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJIS	Criminal Justice Information Services Division (FBI)
CLPE	Certified Latent Print Examiner
COCOM	Combatant Command
CONOPS	Concept of Operations
CPL	Conformance Products List
DAMO-CI	Department of the Army Military Operations – Capability Integration Division
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry
DKO	Defense Knowledge Online
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DOJ	Department of Justice
DOORS	Dynamic Object-Oriented Requirements System
DOS	Department of State
EA	Executive Agent
EBTS	Electronic Biometric Transmission Specification
EM	Executive Manager
FBI	Federal Bureau of Investigation
FORSCOM	U.S. Army Forces Command
FY	Fiscal Year
HIIDE	Handheld Interagency Identity Detection Equipment
HSPD	Homeland Security Presidential Directive
IAFIS	Integrated Automated Fingerprint Identification System
ICE	Immigration and Customs Enforcement
ICSR	Intelligence Community Standards Registry
IdA	Identity Assurance
IDENT	Abbreviation for the DHS, US-VISIT Program's automated biometric identification system

IEC	International Electrotechnical Commission
IED	Improvised Explosive Device
INCITS	International Committee for Information Technology Standards
IOM	Identity Operations Manager
IPMSCG	Identity Protection and Management Senior Coordinating Group
IPT	Integrated Project Team
ISO	International Organization for Standardization
IT	Information Technology
JBOCB	Joint Biometrics Operational Coordination Board
JCIDS	Joint Capabilities Integration and Development System
JESC	Joint Enterprise Standards Committee
JKnIFE	Joint Knowledge Information Fusion Exchange
JTC	Joint Technical Committee
JUONS	Joint Urgent Operational Needs Statement
LISA	Laboratory Information Systems Applications
MARS	Multilingual Automated Response System
MOA	Memorandum of Agreement
MOBS	Mission Oriented Biometric Software
MOC	Memorandum of Cooperation
NEO	Noncombatant Evacuation Operations
NGA	Next-Generation DoD ABIS
NIST	National Institute of Standards and Technology
NSTC	National Science and Technology Council
NVLAP	National Voluntary Laboratory Accreditation Program
ONS	Operational Needs Statement
OPMG	Office of the Provost Marshal General
ORI	Originating Agency Identifier
OSD	Office of the Secretary of Defense
PEO EIS	Program Executive Office Enterprise Information Systems
PM	Project Manager
PSA	Principal Staff Assistant
PTUC	Participating Test Unit Coordinator
RO	Responsible Official (for DoD Forensics)
SCA WG	Standards and Conformity Assessment Working Group
SEEK	Secure Electronic Enrollment Kit
STANAG	Standardization Agreement
TRADOC	U.S. Army Training and Doctrine Command
USAAC	U.S. Army Accessions Command
USAFRICOM	U.S. Africa Command
USCENTCOM	U.S. Central Command
USCG	U.S. Coast Guard
USF-I	U.S. Forces – Iraq
USFOR-A	U.S. Forces – Afghanistan
USSOCOM	U.S. Special Operations Command
USSOCSOUTH	U.S. Special Operations Command South
USSOUTHCOM	U.S. Southern Command
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology Program
VBSS	Visit, Board, Search and Seizure

BIMA FY11 ANNUAL REPORT
Produced by the Communications and Outreach Branch

Editor . . . . . Chris Lawson
Managing Editor . . . . . Mike Klesius
Designer . . . . . Neil Fessler
Contributors . . . . . Steve Taylor
Elizabeth Weaver

Portrait Photographers:
Jeff Wright
McArthur Newell
Jon Girard, US-VISIT
Mass Comms SPC3 Scott Pittman, USN

www.biometrics.dod.mil