



Defense Forensics and Biometrics Agency 2013-2014 Report



CONTENTS

Director's Message

Thank You to Stakeholders

Mission and Vision

Forensics and Biometrics Basics

Organizational Changes

Major Accomplishments

The Bottom Line

The Future

Conclusion

Spotlights

DFBA's MP Connection

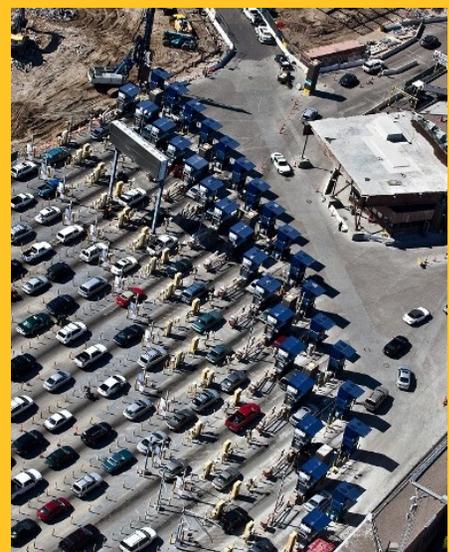
Support to Interagency Missions

NATO Tests Biometrics

Sharing with State Department

Blue Force Biometrics

New DFBA Heraldry



Director's Corner



Thank you for taking the time to read the Defense Forensics and Biometrics Agency (DFBA) 2013-2014 Report. This period has seen major changes at all levels of the organization and the missions which it oversees.

DFBA assumed a new name, moved to a new home, and brought into the fold a new mission—that of forensics. Combining the Department of Defense (DoD) Executive Managers for both forensics and biometrics in one organization within the Office of the Provost Marshal General (OPMG) marks a turning point in both fields—biometrics has finally found a permanent home within DoD, and forensics has been formally recognized as a tool just as valuable on the battlefield as it is to law enforcement. The official union of the forensic and biometric disciplines within a Field Operating Agency ensures DoD will maintain an enduring capability to identify unknown foes.

While DFBA will help DoD maintain training and readiness for the next war, it also will assist other Defense organizations as they implement biometrics in their day-to-day business. Such efforts are

already underway in different services and Combatant Commands, such as access control systems at U.S. facilities in Korea and Qatar and deployable forensic labs for Marine Expeditionary Units. As such efforts continue to develop, DFBA will be there to coordinate standards in support of system interoperability and compliance with DoD policies.

We would not be where we are today without the tireless support of the biometrics professionals in Clarksburg, W. Va; the forensic examiners in Forest Park, Ga., and deployed worldwide; or our headquarters staff in Arlington, Va. Critical support also comes from the Project Manager-Biometrics and the Defense Biometrics and Forensics Office in the Pentagon. Collectively, their work ensures troops in the field have the information they need to accomplish their missions, protect themselves and U.S. assets, and capture both criminals and combatants who mean them harm.

Lastly, OPMG has given DFBA the best possible welcome. Energetic leadership from the Provost Marshal General—currently MG Mark S. Inch, and LTG David E. Quantock previously—has ensured headquarters visibility on forensics and biometrics and the capabilities' future in DoD.

Please enjoy this review of DFBA's first two years. We look forward to many more in the future.

DON SALO, DIRECTOR



A cavalry scout from the 101st Airborne Division uses a Secure Electronic Enrollment Kit (SEEK) to record a villager's biometric data in Shamal District, Khowst province, Afghanistan on January 10, 2013. (U.S. Army photo / Released)



Thank You to Our Stakeholders

DoD Forensics and Biometrics stakeholders come from a wide variety of fields and groups. Just a few examples follow:

- Soldiers, Sailors, Airmen and Marines on the ground in Afghanistan and around the world send us fingerprints and other biometric data they collect to identify known insurgents and terrorists among individuals they encounter on patrol, at access control points, or in other circumstances.
- Physical security and access control professionals across DoD are working to implement biometric solutions within their areas of responsibility.

- Intelligence analysts apply biometric matches to contextual information to identify the enemy and discover trends in hostile groups' behavior.
- Our partner agencies in the Departments of State, Justice and Homeland Security have access to biometric data from the Department of Defense in support of our shared goal of enhancing national security.

A major portion of DFBA's mission is to better engage with you, the stakeholder, in order to anticipate and serve your warfighting and law enforcement needs, and to enable and empower your work.

Top: The 493rd MP Company holds an exercise at Fort McCoy, Wis., March 30, 2014. (U.S. Army photo / Released)

Left: A Sailor descends a ladder during a Visit, Board, Search and Seizure exercise. (U.S. Navy photo / Released)

Right: A piece of an Improvised Explosive Device is examined through a magnifying glass. (U.S. Air Force photo / Released)

Mission and Vision

Mission: DFBA leads, consolidates and coordinates forensics and biometrics activities and operations for the Department of Defense in support of identity operations.

Vision: A DoD Identity Operations Enterprise that protects the nation.

“Commanders in the field have acknowledged two tactical ‘game changers’: constant surveillance from advances in manned and unmanned aircraft, and the application of law enforcement forensic and biometric techniques on the battlefield. These capabilities remove violent extremists’ greatest defense— anonymity.”

LTG Michael Barbero (ret). — former Director, JIEDDO

A coalition forces member collects biometric information from an Afghan Local Police member to ensure his legitimacy in Arghandab district, Kandahar province, Afghanistan, Nov. 4, 2012. (U.S. Navy photo / Released)

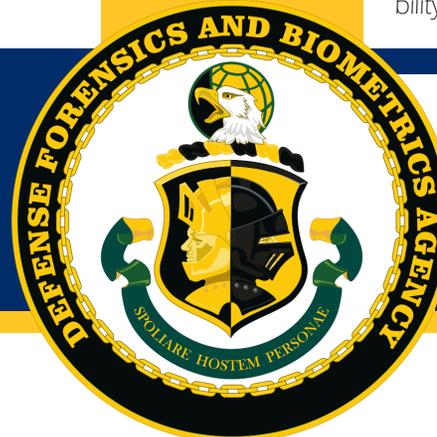
The Problem: ANONYMITY

The Solution: FORENSICS and BIOMETRICS



Employing forensics and biometrics is a three-step process. The first step, **Identify**, strips adversaries of their anonymity on battlefields, at border crossings and other transit points abroad and within the United States. The second, **Enable**, represents the many functions that U.S. Forces can carry out with forensics and biometrics, from compiling watchlists of suspected terrorists to enabling base access for cleared individuals. The third, **Protect**, furnishes the payoff of forensics and 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.

DFBA's predecessor organizations have been performing this role with distinction for a decade, but on an ad hoc basis. DFBA brings forensics and biometrics together in one enduring organization within the **Office of the Provost Marshal General**, an [Army Staff Principal](#) at the Pentagon. DFBA is the Executive Manager for biometrics and most forensics disciplines across DoD (the U.S. Air Force covers digital forensics), a responsibility delegated by the Secretary of the Army.



What are Forensics and Biometrics?

Forensics establishes *facts*; biometrics establishes *identity*.

Forensics, or forensic science, is the discipline of establishing facts that link individuals to other people, places, items or events, often using biometric markers such as fingerprints and DNA. It describes both the tools and techniques of the investigation process, from collecting evidence in the field to comparing samples in a sterile lab. The Latin root of the word refers to using evidence to argue before a legal forum.

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

- Fingerprint
- Palm print
- Facial recognition
- Iris recognition

The term "biometrics" also refers to the process of using automated methods, such as DoD's Automated Biometric Information System (ABIS), to recognize individuals based on these and other characteristics. Biometrics researchers continue to enhance the usability of well-known modalities, such as DNA, analyze potential for behavioral modalities, such as gait, and write new search algorithms to increase the speed and accuracy of biometric matches for users in the field.



Above: A DNA examiner adds chemical reagents to a tube containing a possible DNA sample at the Afghan Captured Materials Laboratory at Bagram Air Field, Afghanistan. (CJTF Paladin photo / Released)

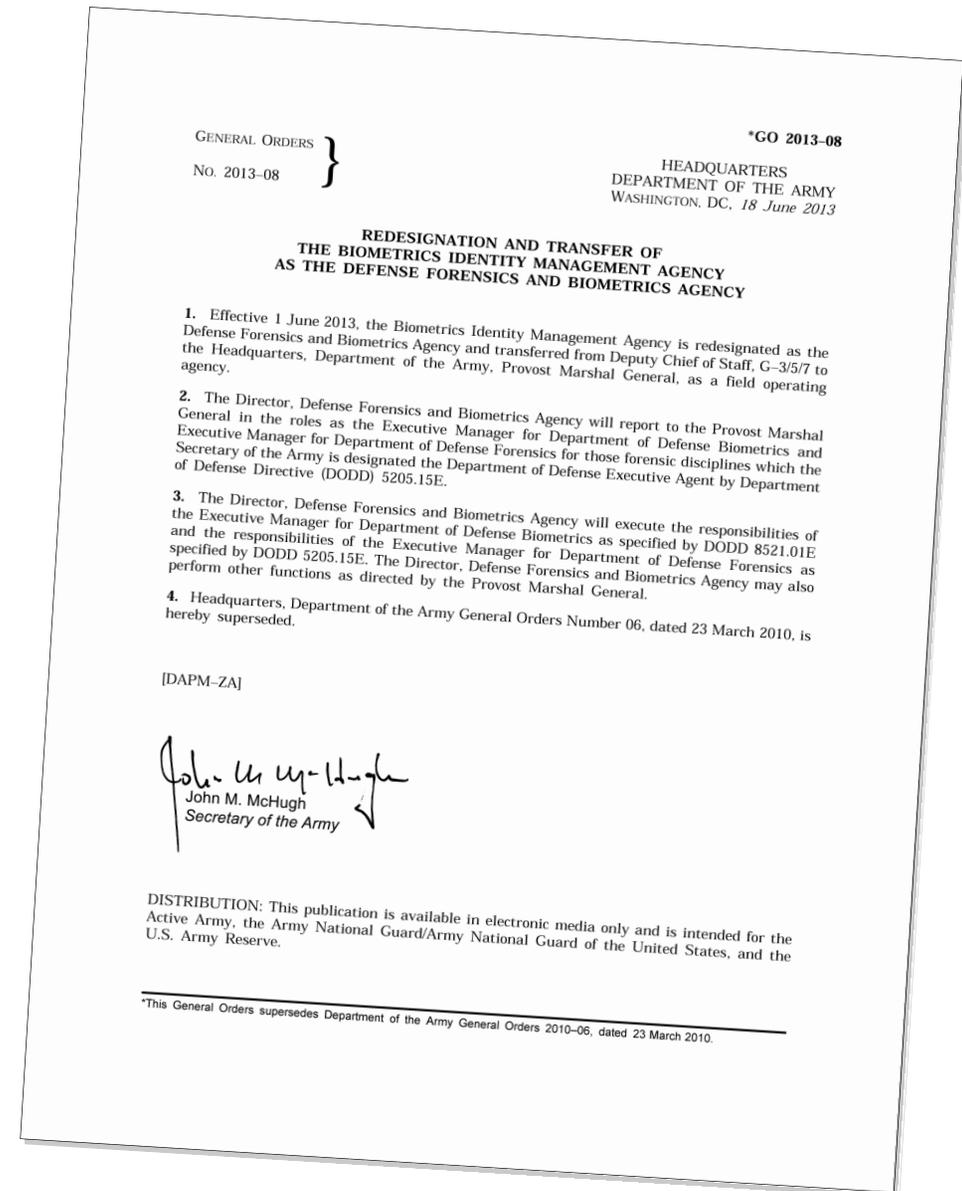


Above: A Soldier uses a SEEK II device to record the irises of a local man in the Panjwa'i District of Afghanistan in support of Operation Enduring Freedom. (U.S. Army photo / Released)

Organizational Changes

DFBA Becomes a Field Operating Agency

The Department of the Army General Order (DAGO) 2013-08, signed by the Secretary of the Army (SecArmy), created a new Field Operating Agency by redesignating the former Biometrics Identity Management Agency (BIMA) as the Defense Forensics and Biometrics Agency (DFBA). The order, effective 1 June 2013, merged forensics and biometrics under a single executive manager and gave the organization a permanent home in the Office of the Provost Marshal General (see next page for more on the PMG). The long process began in 2000 when Congress designated SecArmy the Executive Agent for DoD Biometrics. Over the ensuing decade, biometrics shifted from the information technology community to front-line warfighters in various ad hoc organizations. When the Provost Marshal General, already Executive Manager for DoD Forensics, took on biometrics in late 2012, the biometrics organization was renamed DFBA and assigned responsibility for both complementary disciplines. Its status as a Field Operating Agency ensures that DoD forensics and biometrics will endure.



Above: The text of DAGO 2013-08.
Left: 14th Provost Marshal General MG (now LTG) David Quantock ceremonially cuts the cake at [DFBA's Uncasing Ceremony](#) while DFBA Director Don Salo looks on. DFBA's newly-uncased colors are at right. (U.S. Army photo / Released)

Organizational Changes



DFBA Joins the Military Police

As part of becoming a Field Operating Agency, DFBA was placed within the **Office of the Provost Marshal General (OPMG)**. The [Provost Marshal General \(PMG\)](#), currently [MG Mark S. Inch](#), is the Army's "top cop" and the principal military advisor to the Secretary of the Army and Chief of Staff of the Army on policing matters. The PMG is the Commanding General of Army Corrections Command and Criminal Investigation Command, and executes SecArmy's Executive Agent responsibilities for several law enforcement-related fields, including [forensics](#) and [biometrics](#). These responsibilities were further delegated to DFBA.

BIMA Becomes an "Activity"

BIMA was dissolved as an Agency by DAGO 2013-08, but the name lives on as the Activity responsible for operating the DoD's authoritative biometric database—ABIS—and synchronizing it with outside systems. The **Biometrics Identity Management Activity** in Clarksburg, W. Va., stores, matches, and shares biometric data collected worldwide in accordance with mission requirements. BIMA technical experts also assist interagency and international partners with ABIS interoperability and building new biometric databases. BIMA spent much of 2013 and 2014 upgrading from ABIS 1.0 to **ABIS 1.2**.



Forensics Integration

As Executive Manager for Forensics, DFBA works closely with the **Defense Forensic Science Center (DFSC)**, a part of [U.S. Army Criminal Investigation Command](#), as well as with the Navy and Marine Corps, which maintain expeditionary forensic capabilities. DFSC includes the U.S. Army Criminal Investigation Lab (USACIL) and the Forensics Exploitation Directorate (FXD). USACIL is the central forensic lab for investigative needs from across DoD. FXD is a network of deployable labs that provide on-site forensic support to Combatant Commanders.



DFBA's Military Police Connection

Although DFBA is only two years old, its mission goes back considerably further. Military forensics—that is, for law enforcement purposes—began during World War II. From its inception, forensics has been a Military Police mission, executed today by the Defense Forensic Science Center (DFSC). As a complementary field, biometrics has also been an Army responsibility ever since forward-thinking leaders in 2000 assigned the Secretary of the Army as the DOD Executive Agent for biometrics, even before it was a common-place technology.



As a Field Operating Agency within OPMG, DFBA reports to MG Mark Inch, 15th Provost Marshal General. (U.S. Army photo / Released)

The fusion of forensic and biometric skill sets in the field created a new military capability—identity operations—to deny anonymity to adversaries by matching them to their biological traces in a tactically-useful timeframe. DFBA is the enduring organization to fully develop this capability.

The Military Police Corps is well-suited to the forensic and biometric missions, with ready applications across the many roles that MPs fill. MPs are the Army's experts at such wide-ranging tasks as collecting latent fingerprints, managing detainees or controlling post access. Forensics and biometrics connect each of these missions, enhancing the capabilities of each by facilitating the flow of identifying information across the whole. DFBA makes it possible.



Organizational Changes

New Interagency Biometrics Facility

BIMA will be relocating to the **Biometrics Technology Center (BTC)** in 2015, a new facility near Clarksburg which it will share with the FBI.



The new building, currently under construction, is designed to house data centers and the personnel to operate them. The BTC will provide a permanent home to BIMA and the DoD's authoritative biometric repository.



Artist's rendering of the future Biometric Technology Center.

Collectively, these changes administratively demonstrate the operational integration of forensics and biometrics across the interagency domain. Biometric databases and portable devices enable forensics to provide immediately actionable identity intelligence when latent prints are recovered from sensitive sites or equipment. Ongoing software upgrades from ABIS 1.0 to ABIS 1.2 ensure collaboration will remain as fast and effective as possible for years to come. The co-location of DoD and DOJ biometric assets will have a similar effect on interagency cooperation.

A coalition force member collects biometric data during a security operation in Nahr-e-Saraj district, Helmand province, Afghanistan, February 2013. (U.S. Army photo / Released)





A Soldier provides a Border Patrol agent a tour of the motor pool as part of logistical support to border control efforts in Arizona. (U.S. Army photo / Released)

Major Accomplishments

Interagency Cooperation

Interagency datasharing capabilities have dramatically improved since DFBA's inception, ensuring that hostile individuals encountered abroad will be swiftly identified at U.S. borders. Examples include:

Customs and Border Protection (CBP), a part of the Department of Homeland Security (DHS), shares a direct connection with DoD ABIS, resulting in an average of more than 2,000 submissions per day.

The FBI Criminal Justice Information Services Division's (CJIS) Global Initiatives Unit (GIU) has shared more than 1.5 million biometric files collected worldwide from criminal and terrorism-related cases.

A joint Memorandum of Understanding between DoD, the FBI and the State Department was established for the sharing of biometric enrollments from Diplomatic Security Services (DSS) employment vetting, criminal and counterterrorism cases. Since early 2014, the Department of State has transmitted more than 20,000 records to ABIS for screening of Special Immigrant Visa applicants for past terrorist or criminal affiliation. The State Department's Bureau of Counterterrorism also submits files to ABIS. Thousands of applicants have been denied entry to the U.S. as a result.

DHS' **Office of Biometric Identity Management (OBIM)** includes DFBA on its Executive Steering Board (ESB), along with representatives from the Departments of State and Justice. The ESB meets quarterly to discuss DHS biometric efforts and coordinate OBIM's interagency support.

DFBA is a non-voting member of the **Identity Intelligence Board of Governors (I2BOG)**. Composed of organizations across the Intelligence Community (IC), including DoD intelligence bodies, the I2BOG meets quarterly to discuss identity intelligence and coordinate IC-wide strategic and technological efforts. The Office of the Undersecretary for Defense, Intelligence (OUSDI), is DoD's voting board member.

The **JIEDDO Seniors Community of Action Board** includes DFBA as a member. The board meets quarterly to discuss counter-improvised explosive device (C-IED) operational activities across the globe. Representatives include agencies from across the US Government and foreign allies.

DoD Biometric Data Supports Interagency Missions

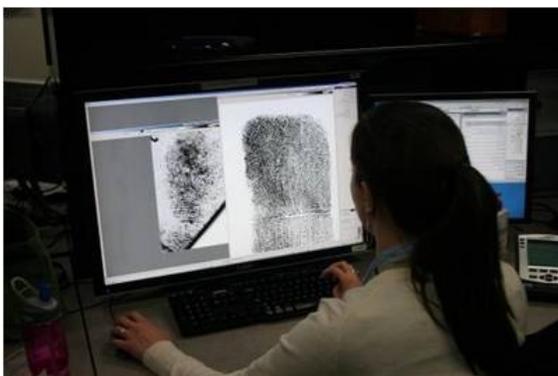


On 26 December 2013, U.S. Customs and Border Protection (CBP) apprehended a group of 17 individuals in Falfurrias, Texas. The individuals' biometrics were compared with U.S. Government databases, and DoD ABIS contained two positive biometric matches with enrollments from prisoners in El Salvador. These biometric matches were forwarded to CBP's National Targeting Center (NTC) for further investigation.

The Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) unit in El Salvador confirmed both of the subjects in custody were prison escapees wanted for murder. CBP Falfurrias Station coordinated with HSI to facilitate interviews and extradition to El Salvadorian authorities once their U.S. sentences are completed.

The Federal Bureau of Investigation successfully apprehended a man attempting to pick up a drug shipment at Entebbe Airport in Uganda on 28 August 2013. To confirm the subject's identity, the FBI team biometrically enrolled him and found matching biometrics in DoD ABIS. The subject had been previously enrolled in 2012 as a foreign nation hire at a Coalition facility in Afghanistan. The arrest highlighted the ability of U.S. law enforcement personnel to query DoD ABIS and apply its information to their mission, even when abroad.





A latent print examiner at BIMA compares two submissions to establish or rule out a match. (DFBA photo / Released)

UV14 Tests NATO Tools



Hosted at Ørland Main Air Station, Norway, Unified Vision is a biennial technology demonstration designed to test new tools in NATO's ISR arsenal. This year, [Unified Vision 2014](#) (UV14) demonstrated the

feasibility of multiple NATO-member nations collecting and sharing biometric data in a unified NATO system. DFBA led the effort to write technical standards for all NATO members, and provided guidance for implementing the standards in NATO's internal biometric database.

The biometric scenario featured four threat cell networks using IEDs to carry out attacks on NATO forces. The NATO Special Operations Headquarters' (NSHQ) Forensics Lab and The Netherlands' Forensics Van conducted technical exploitation of items recovered from a safe house, IED events, and individuals encountered during operations. Biometric samples recovered from items were matched against records from prior encounters with individuals. Data gathered were then synthesized into a Biometric-Enabled Watchlist (BEWL) for the use of troops in the field.

Major Accomplishments

International Initiatives

DFBA has engaged with partner nations in cooperation with the Departments of State, Justice and other arms of the U.S. Government. These initiatives improve the capabilities of U.S. allies and contribute to a defense-in-depth of our own borders. Examples include:

DFBA provided vital support to the **NATO Biometrics Program of Work (POW)**, the body charged with implementing the NATO Biometrics Framework enacted in 2012. DFBA gathered inputs from the U.S. and other NATO mem-

bers to NATO Standardization Agreement (STANAG) 4715, and served as lead editor on the final product released in October 2013. These efforts culminated in Unified Vision 2014, a biennial NATO technology demonstration which featured biometric capabilities for the first time. DFBA's Standards Branch assisted NATO with creating security SOPs for the safe handling of biometric data during the exercise, in addition to STANAG development. The Enterprise Engagement Branch also provided support with U.S. European Command collaboration and Strategic Communications efforts. See details in sidebar, left.



U.S. Marines conduct Sensitive Site Exploitation training with their counterparts in Gabon in June 2014. (U.S. Marine Corps photo / Released)

State Department Screens Immigrants with Biometrics



DFBA, the FBI and the State Department have collaborated to enable biometric screening of Special Immigrant Visa (SIV) and U.S. Refugee Admission Program (RAP) applicants. Individuals who apply for visas under either program have their biometrics compared with ABIS records. Of more than 20,000 submissions in the program's first six months, about half produced ABIS hits. Most were innocuous, but many applicants were matched to criminal or terrorist histories in Iraq or Afghanistan. The following examples are from just one two-month period:

- 08 June 2014: An individual detained in 2007 by Coalition Forces in Afghanistan was biometrically identified as a threat and denied a visa under the SIV program.
- 19 June 2014: A SIV applicant from Iraq was flagged when his biometrics matched a record on the Biometric-Enabled Watchlist (BEWL). He had been added to the list for terrorist affiliation in March 2014.
- 23 June 2014: An individual considered a criminal threat and banned from U.S. bases in Afghanistan applied for a U.S. visa under the SIV program. He was identified via biometrics and denied entry.
- 29 June 2014: A subject added to the BEWL in 2010 for terrorist affiliation was identified through SIV screening four years later. He was denied a visa.
- 07 August 2014: An Afghan subject placed on the BEWL in 2013 for terrorist connections was identified on his second application to the SIV program and denied a visa.

Major Accomplishments

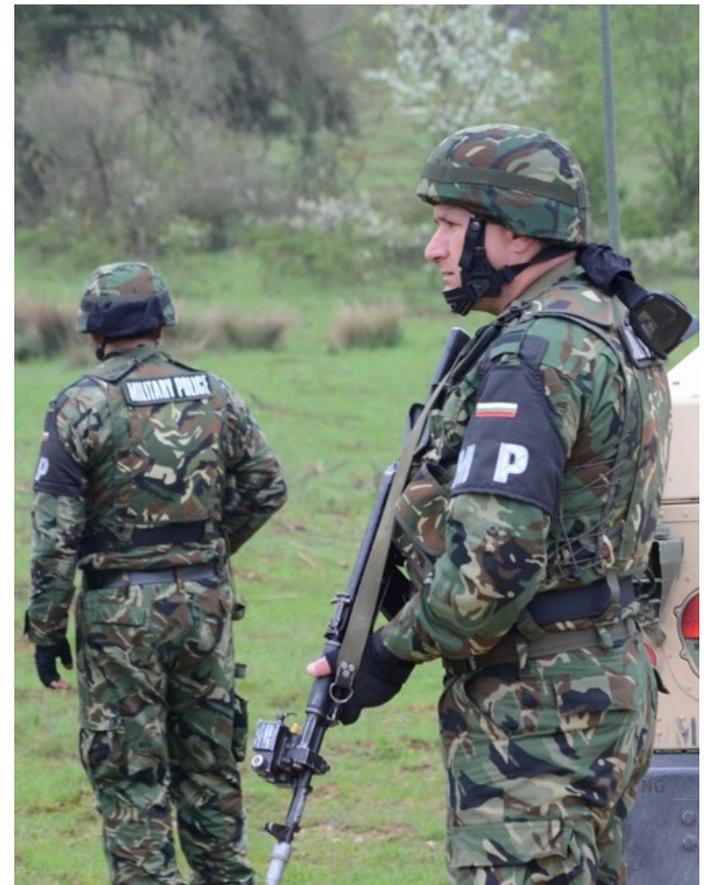
DFBA conducted [ongoing engagement](#) with the **American, British, Canadian, Australian and New Zealand (ABCA) Armies Program**, attending annual meetings and providing distance support to standardization efforts. DFBA advocates for U.S. and U.S. Army positions in such engagements, and also leads technical discussions and task development. The cumulative effect of DFBA's efforts improves interoperability with our closest allies as they build their own forensic and biometric capabilities.

Engagement with Kosovo resulted in acquisition of more than 15,000 unsolved latent prints and in excess of 60,000 ten-print records which, when ingested into DoD ABIS, resulted in numerous watchlist hits and matches to unresolved latent prints. Biometrics supports the force protection and intelligence efforts of the several hundred U.S. troops still serving alongside NATO allies in Kosovo.

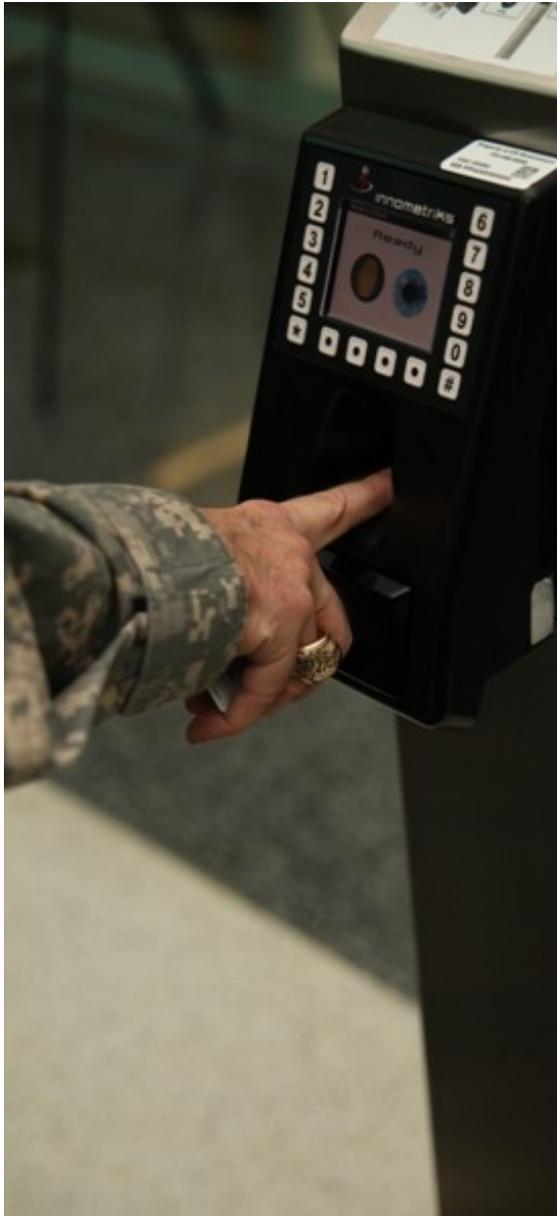
Experts from BIMA helped the **Federated States of Micronesia (FSM)** establish a domestic biometric database in late 2013. Working with the FBI and [Joint Interagency Task Force West \(JIATF-W\)](#), BIMA performed a needs assessment for the FSM's Secretary of Justice and biometrically en-

rolled a segment of its prison population to provide a baseline data set while the system is built.

DFBA has also played important roles in **inter-agency standardization and policymaking**, helping chart a path for the entire U.S. Government as biometrics becomes a common tool.



Above: Bulgarian MPs maintain security during a NATO Kosovo Force (KFOR) exercise. (U.S. Army photo / Released)
Left: U.S. and Australian personnel provide forensic training to an Afghan police recruit. (U.S. Army photo / Released)



Biometric access controls are demonstrated at the DoD's Mark Center in Alexandria, Va., in January 2014. (Pentagon Force Protection Agency photo / Released)

Major Accomplishments

Standards & Architecture

The Forensics and Biometrics Standards Working Group (FBSWG) charter was formalized in July of 2014. The FBSWG develops recommendations to facilitate and promote DoD interests within national and international forensics and biometrics standards organizations. It also enhances awareness across DoD of external standards development activities. This ensures the current, enduring, emerging and future needs of operational commanders and other stakeholders are reflected in the standards development process.

The Forensics Enterprise Architecture Working Group (FEAWG) was formed in October 2013 to establish a way forward for a DoD Forensics Enterprise Architecture, and to facilitate the resolution of interoperability, data reuse, and data and information sharing issues through architecture. The FEAWG has participation from the Intelligence and Maneuver Support Centers of Excellence, TCM-BF, Army G-2, DFSC, FBI, Defense Cyber Crime Center (DC3), Air Force Office of Special Investigations (AFOSI), and the Unified Exploitation Proponency Office Requirements Determination Division (RDD) Capabilities Development and Integration Directorate (CDID) and U.S. Army Combined Arms Center (CAC).

"Credentialed" Biometrics: A Growing DFBA Mission

The world is changing; as high-end wartime conflicts draw down, security efforts at home step up. With that in mind, DFBA added applications for credentialed personnel within the Business Mission Area (BMA) to its portfolio through the Business Functions Branch (BFB) in 2013 and 2014. The Branch led DFBA policy integration efforts, participating in the Army Identity Strategy Working Group.

The Branch worked with the Office of the Undersecretary of Defense (Policy) to assist with the integration and inclusion of business functions in policy issuances, such as DoD Directives, Instructions and directive-type memorandums. It was focused on moving the Enterprise from a wartime mindset to that of institutionalizing forensics and biometrics capabilities within DoD. However, this was and continues to be a whole-of-DFBA effort as projects are identified and initiatives are taken to integrate biometrics into logical and physical access.

Among current initiatives, biometrics are a piece of the [Pentagon Force Protection Agency's](#) (PFPA) transition from the Pentagon access badge to the Common Access Card (CAC) over the coming year. The groundwork for the change was laid by funding from DFBA's predecessor organization.

Elsewhere in OPMG, Army Corrections Command (ACC) has expressed an interest in incorporating biometrics into its operations. ACC and DFBA have been jointly researching and visiting local, state and federal correctional facilities to see examples of biometric integration. The first visits were to Pinellas County Jail in Clearwater, Fla., and the Naval Consolidated Brig (NCB) in Charleston, S.C. The DFBA team also visited the Fairfax County, Va., offices of the Northern Virginia Regional Identification System (NOVARIS). This computer network links the fingerprint records of Maryland, Northern Virginia and Washington, D.C.

Institute of Heraldry Creates DFBA Seal and Flag

When DFBA was established as a Field Operating Agency, it became eligible for official heraldry, including a seal and flag. The Army's Institute of Heraldry produced the design in early 2014.

The seal is highlighted by two helmets joined back-to-back, with one visor up and another visor closed. They symbolize DFBA's ability to reveal the identities of individuals trying to stay hidden. The green and gold scroll connects DFBA to the colors of the Military Police Corps, of which it is now a member, and the Latin motto translates as "Deny the Enemy Anonymity." For more details, you may visit the [Institute's description online](#).

The Institute of Heraldry, located at Fort Belvoir, Va., was officially established in 1919, but traces its lineage back to the designers of the Medal of Honor during the Civil War. Today, among its other duties, it is the only source for official Presidential and Vice Presidential seals.



Above: The design of DFBA's new colors, courtesy of the Institute of Heraldry. (U.S. Army graphic / Released)

Major Accomplishments

Strategy & Policy

DFBA worked with OPMG to incorporate forensics and biometrics into the **MP 2020 Strategic Plan**. [Goal 3.5](#) issues a call to "Integrate biometrics and forensics technologies and capabilities." Both disciplines contribute to the overall concept of identity, and are vital to denying the enemy anonymity while also creating opportunities to enhance internal DoD functions.

DFBA contributed to other **Army planning documents** in addition to MP 2020, including the Army Planning Priorities Guidance, the Army Campaign Plan. Further, the Plans staff worked closely with the community of interest and the Defense Biometrics and Forensics Office to create and deliver draft DoD Directive 8521.01E and draft DoD Instruction 5225.7C. Both documents establish policy, assign responsibility, and provide direction to the enterprise.

The DFBA policy team was able to process the DoD Biometric Repository's **System of Records Notice (SORN)** and **Privacy Impact Assessment**, and work biometric data-sharing with DoD's Program Manager-Biometrics. The Privacy Act of 1974 and Paperwork Reduction Act require each agency to publish notice of its systems of records in the Federal Register. In addition, the policy team was able to establish data-sharing procedures between the organization and various Combatant Commands, Services, Agencies, and Interagency partners.

Right: A Marine performs Sensitive Site Exploitation on an insurgent position following a firefight in Helmand province, Afghanistan, in July 2014. (U.S. Marine Corps photo / Released)

A Nation Protected

The **end result** of DFBA's activities is the identification of hostile parties and the prevention of hostile acts. Some recent examples follow:

Biometrics prevented a **potential insider attack** by a former detainee despite deformities he suffered following his release. In 2009 the subject was initially detained and biometrically enrolled by Coalition Forces in Afghanistan, and he was subsequently linked to Improvised Explosive Device





Major Accomplishments

(IED)-related activity. In between these two encounters, he suffered burns to his face and required multimodal biometrics to identify. Finally, in June 2013 he applied for on-base employment, but was denied access when biometrics linked him to his prior adverse encounters.

A **Taliban defector** was identified by SOCOM elements equipped with biometric kit. In 2011 the subject joined the Afghan National Police and enrolled his biometrics. After being promoted to commander of a checkpoint in 2012, he defected to the Taliban, providing weapons and other support. During a targeted raid in September 2013, SOCOM detained and identified the subject, removing him from the fight.

An Iraqi using multiple avenues to enter the U.S. was biometrically identified through **interagency cooperation** and denied visas both times. The subject was a Coalition Forces host-nation hire in Iraq and was enrolled in ABIS in 2008. He was later connected to insurgent activity and denied a Special Immigrant Visa (SIV) by the State Department in 2011. He later went through screening by U.S. Citizenship and Immigration Services and enrolled his biometrics with DHS. Again, he was denied after being identified.

Biometrics identified a former host-nation hire who went **AWOL**. After being hired by Coalition Forces in Afghanistan in 2007, the subject was nominated to the Biometric-Enabled Watchlist (BEWL) in 2010 after long periods of unexplained absence. He was suspected of travel to several countries and provided inconsistent an-

swers about his whereabouts. In April 2014, he attempted entry to the U.S. under the SIV program, but was denied after being biometrically linked to his DoD ABIS record.

An **individual deported from the U.S.** multiple times since 1996 was biometrically identified by Customs and Border Protection in Puerto Rico. A native of the Dominican Republic, the subject was deported repeatedly for immigration and drug charges from both the continental U.S. and Puerto Rico over several years. After undertaking an illegal voyage to Puerto Rico in late 2012, he was added to the BEWL. The subject's BEWL record was identified when he was next encountered in Puerto Rico in August 2014. Customs and Border Protection denied the subject entry to the territory.

In October 2014, the **August Vollmer Excellence in Forensic Science Award** was awarded to the Defense Forensic Science Center by the International Association of Chiefs of Police (IACP) in the category Significant Investigative Value in a Major Crime. The forensic examiners, analysts and operations support staff of DFSC's Forensic Exploitation Directorate (FXD) were directly responsible for the collection, preservation and exploitation of evidence leading to a conviction in an Afghan court and the first-ever death sentence of an Afghan National linked to insurgent activity; specifically, the attack on Camp Bastion and Camp Leatherneck on 14 September 2012 in which two U.S. Marines were killed. The award recognizes DFSC's contribution to the law enforcement and forensics communities (see photo, left).



Top left: A U.S. Army Criminal Investigation Command Special Agent processes a crime scene with an alternate light source. (U.S. Army photo / Released)

Bottom left: DFSC's Johnny Holley (L) and Archie Tabor (R) accompany Provost Marshal General MG Mark Inch to accept the August Vollmer Award in October 2014. (IACP photo / Released)

The Power of ABIS

More than...

12,000,000 submissions since 2004

6,000,000 unique identities stored

5,000,000 matches since 2004

3,000,000 identities added in FY13-14

1,500,000 matches in FY13-14

12,000 matches of watchlisted or top-tier threats since 2011

Forensic Exploitation Directorate: Success in Afghanistan

Between 2012 and 2014:

860,000 exhibits processed by FXD

57,000 fingerprints added to DoD ABIS

20,000 individual cases

2,800 identities added to BEWL

900 Prosecution Support Packages

485 convictions in IED-related cases

The Bottom Line

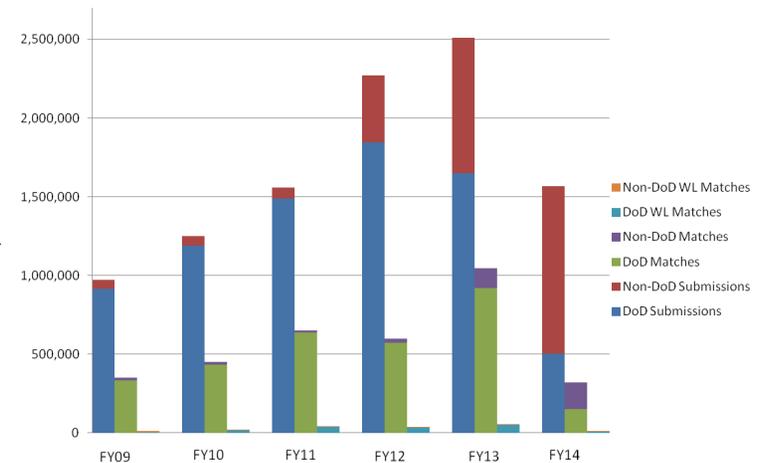
DFBA provides information crucial to identifying threats.



A Military Police Soldier enrolls a detainee on a biometric device. (U.S. Army photo / Released)

Composition of ABIS Records

DoD submissions (blue) peaked in 2012 and have declined as operations in Afghanistan have drawn down, but interagency requests (red) are growing fast as datasharing steadily improves. Whatever the mission, ABIS stands ready to support.



Looking Ahead

Although the combat role of forensics and biometrics will be curtailed as U.S. forces draw down in Afghanistan, they will become more visible in other operations. Demands on the DoD biometric database will shift from large-scale counterinsurgency to smaller operations worldwide, from support to Special Operations to Navy boarding parties at sea.

DoD will remain at the forefront of biometric and forensic technology. Efforts are already underway to implement biometric access at the Pentagon and other major installations. DFBA will make such tools more common across DoD.

The Biometrics Identity Management Activity will move to a new location in West Virginia, which it will share with the FBI's Biometric Center of Excellence. This will enhance interagency cooperation and the ability to share critical information between departments.

Conclusion

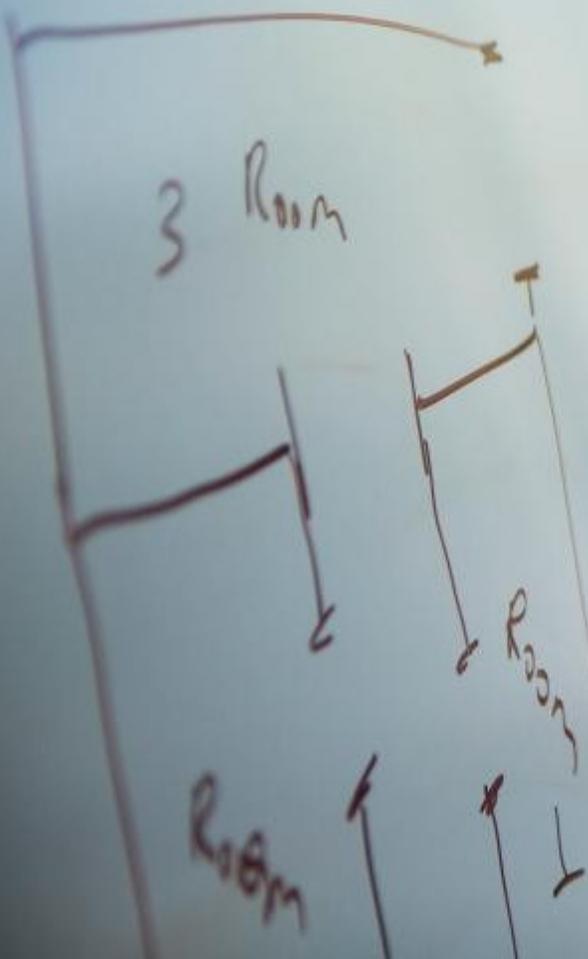
DFBA provides enduring forensics and biometrics capabilities to the Department of Defense.

Lessons learned in the deserts of Iraq and mountains of Afghanistan will not be forgotten. Forensics and biometrics proved themselves as battlefield tools and robust technologies, and DFBA will ensure this experience is retained and built upon. DFBA will maintain forensics and biometrics as enduring capabilities, integrating them into day-to-day business processes as well as warfare doctrine. When the next fight comes, forensics and biometrics will be ready.

A Soldier enrolls an Afghan civilian during Operation Alamo Scout 13, in Kandahar province, Afghanistan, on Feb. 12, 2014. (U.S. Army photo / Released)

SSE

Sketch



Product of
**Defense Forensics
and Biometrics Agency**
Enterprise Engagement Branch

www.dfba.mil