SIGNAL ONLINE
More than a magazine: We're AFCEA.

# U.S. Defense Department Expands Biometrics Technologies, Information Sharing

*By George I. Seffers, SIGNAL Magazine*
**October 2010**

Sgt. Michael Weaver, USMC (l), Personal Security Detail, Regimental Combat Team 5, uses the Biometric Automated Toolset just north of Al Qaim, Iraq, to enter an Iraqi man's information into a national database.

Agency seeks to replace current methods, conduct more efficient data collaboration among departments.

The U.S. Biometrics Identity Management Agency, an Army agency tasked with coordinating biometrics efforts across the Defense Department, is expanding capabilities and broadening data sharing with other government agencies and coalition partners. The agency, which also operates the department's premier biometrics database, is coordinating with the departments of Justice, State and Homeland Security to share biometrics data between the three primary databases used by the various departments.

The Defense Department relies on its Automated Biometrics Identification System (DOD ABIS) to process and store biometrics data from foreign nationals requesting access to U.S. installations overseas, latent prints from improvised explosive devices and other hostile actions, enemy combatants and detainees. The Justice Department uses the Integrated Automated Fingerprint Identification System, which includes not only fingerprints but also corresponding criminal histories; mug shots; scar and tattoo photographs; physical characteristics such as height and weight, hair and eye color; and aliases. The system also includes fingerprints, mostly of individuals who have served or are serving in the U.S. military or have been or are employed by the federal government.

The departments of State and Homeland Security share a database, which like the Defense Department system also is known as the Automated Biometrics Identification System. It is referred to as IDENT, and it stores biometrics from visa applicants, visitors to the United States, illegal border crossers and immigration violators.

Government agencies have been widely criticized, especially in the aftermath of the terrorist attacks on September 11, 2001, for not sharing data that would enable intelligence analysts to connect the dots. "The person we may collect biometrics on in [the war] theater today may be the same person who shows up in a U.S. airport wanting entry—and this has happened," explains Lisa Swan, deputy director of the Biometrics Identity Management Agency. "Maybe he gives the same name, maybe he doesn't. Maybe he links back to a fingerprint that was found on an improvised explosive device. That's certainly something you want to know before you let someone in the country.

"We're working with our interagency partners to share data where policy allows and building the technology solutions to make that easier so that we can increase national security across the board," she notes. "DOD is sharing data between those three departments now on a somewhat limited basis. Between DOD and the FBI, we have good sharing. With our other partners, we're sharing some but it's

still cumbersome and limited. We're all committed," Swan emphasizes, "to working toward what we're referring to as the 'biometrics triad,' which will link those three databases so that information coming in gets automatically shared with the right people at the right time."

By improving those data-sharing capabilities among departments, the government more fully is realizing the power of biometrics technology, Swan says. "The power of biometrics is being able to share it."

The agency also is seeking a replacement for the DOD ABIS. The replacement is called the Biometrics Enabling Capability. It will be an official program of record that will offer greater capacity and throughput, as well as expand the types of biometrics data stored, possibly including voice recognition, DNA and body odors, Swan says. DOD ABIS is known as a quick reaction capability and is not a program of record. The military relies on DOD ABIS to support operations Enduring Freedom and Iraqi Freedom. The system provides a central, authoritative repository for biometric records. It became operational early last year and stored only fingerprints.

The system has since been upgraded to DOD ABIS version 1.0, which stores facial images, palm prints and iris patterns in addition to fingerprints. Version 1.0 also includes a more advanced algorithm that uses a combination of partial matches from multiple biometric sources—a partial fingerprint combined with a partial palm print, for example—increasing the likelihood of a match. And it does so nearly 30 times faster than the original system.

"Programs of record are formally recognized acquisition programs that go through development and full life-cycle support. That is not what we have today. It is what we are working toward. The DOD ABIS we have today has significantly more capability than the one we had two years ago. The new system will have significantly more capability than we have today," Swan says. "As we do this interagency and international data sharing, we will need more computing power and the ability to search more records quickly. I think Biometrics Enabling Capability will also bring enhancements as far as continuing to add modalities—fingerprints, face, voice, foot smell, whatever the next one might be."

The various tools used to collect biometrics data on the ground also are due for replacement by next-generation technologies under another program of record designated the Joint Personnel Identification System. This technology potentially could add the capability to gather such data as voice recognition and foot odor identification data for inclusion in the new Biometrics Enabling Capability database.

Sgt. Major Robert Haemmerle, USA, assigned to the Biometric Task Force, demonstrates how to use the Handheld Interagency Identification Detection Equipment (HIIDE) device to Afghan National Army soldiers at Camp Tombstone, Helmand province, Afghanistan. The HIIDE system is a multimodal biometric system that collects and compares fingerprints, iris and facial photos against an internally downloaded biometric watch list.

In addition to identifying and tracking insurgents, biometrics tools are used to protect U.S.-controlled military installations at various locations across Southwest Asia, so that stolen or counterfeited badges no longer pose the threat they once did. Visitors entering a protected base or facility now swipe their badges through a reader while simultaneously placing a finger on a fingerprint scanner. The scanner and reader are part of the Biometric Identification System for Access, which ensures the identities of those with legitimate access. Non-U.S. citizens seeking employment on U.S. bases are among those required to use the system. Upon applying, potential employees must submit their biometric and biographic data. If the information does not match known persons of interest, the applicant may receive a card and employment.

The Biometric Automated Toolset (BAT) and the Handheld Interagency Identity Detection Equipment (HIIDE) system also are used in Iraq and Afghanistan. The Army's Battle Command Battle Laboratory, Fort Huachuca, Arizona, developed BAT in 1999 to deal specifically with the problem of local nationals in

the Balkans who were causing problems on one U.S. installation, being barred from re-entry and moving on to another installation. At the time, no system existed for tracking rabble-rousers from one installation to another. BAT includes a handheld iris scanner, digital camera and fingerprint reader with a laptop computer and identification processing software. The computers connect to a series of servers and regularly update biometric records. The system compares fingerprints, iris images and facial photos used to enroll, identify and track non-U.S. persons of interest.

Workers at Tobyhanna Army Depot, Pennsylvania, recently assembled more than 100 BAT toolset kits for shipment to Southwest Asia. Last year, warfighters requested a simplified BAT design to provide easier access to the components, cut down on the number of parts to assemble and keep the system operational in extreme temperatures. Inspired by a prototype designed by a soldier in Afghanistan, Tobyhanna workers came up with a new design consisting of a hardened case, two layers of foam separating and protecting the power cables and cords, and a laptop cooler that forces air into the power supply bay, dissipating the heat buildup.

In use since 2007, HIIDE is a small, handheld device for collecting and matching iris scans, fingerprints and facial scans. More portable than BAT, it collects biometric, biographic and contextual data on persons of interest and matches it against the BAT database. HIIDE warns the user if a person being checked is on a watch list, and it can create tracking reports of biometric encounters for later intelligence analysis.

The Biometrics Identity Management Agency is endeavoring to deliver even more sophisticated biometrics tools in support of the war effort. It is working with industry on development of a proposed fluttering-shutter camera system to acquire high-quality images from moving subjects. Based on computer photography concepts that utilize fluttering patterns during image capture to aid in image deblurring, the technology is designed to improve the capture of high-quality images in non-ideal conditions. Uncooperative subjects and environmental conditions compound motion effects, causing problematic blur in image processing and matching. This is the case particularly for handheld biometric platforms where both the subject and operator may be moving. The prototype system integrates both flutter shutter and deblurring technology in iris scanning devices.

Another prototype uses multiple scanning lasers and tracking algorithms to correct for subject motion while an image is being taken. This prototype also employs infrared imaging to capture 3-D facial images at night and within poorly lit environments and captures a person's heartbeat pattern at the same distance, which could signal high stress levels in someone about to create trouble. In addition, the University of West Virginia is working with the agency on a new approach to fuse and dynamically update biometric data from multiple technologies, improving accuracy and performance.

"We look at what's going on in biometrics science and technology across the department and in academia to see where we can leverage the different activities and pull them together for the greater good," Swan explains.

Formerly known as the Biometrics Task Force, the Biometrics Identity Management Agency in March became a full-fledged U.S. Army agency with a departmentwide mission. The secretary of the Army is the Defense Department's executive agent for biometrics, so he is responsible for coordinating biometrics activities across the department, and the agency executes those activities on his behalf.

Swan foresees a time when biometrics data is used to identify friendly or enemy troops wounded on the battlefield, to ensure soldiers and their families receive authorized health care, and to identify displaced persons or track individuals who have received emergency rations following a natural disaster.

**WEB RESOURCE**
*U.S. Biometrics Identity Management Agency: www.biometrics.dod.mil/default.aspx*