


DAPKUS

## DOD Biometrics—Lifting the Veil of Insurgent Identity

Jody Kieffer and Kevin Trissell

**E**very day thousands of people report to work on U.S.-controlled military installations in Southwest Asia. Today, Soldiers and Marines who guard these facilities rely on increasingly sophisticated biometric tools for identity information that protect them, their facilities, and local populations from harm.

SGT Eric Dapkus, 2nd Battalion, 1st Infantry Regiment, 5th Stryker Brigade Combat Team (BCT), 2nd Infantry Division, uses a HIIDE device during a cooperative medical engagement in the Maiwand District, Hatal, Afghanistan, Jan. 16, 2010. (U.S. Air Force (USAF) photo by SSG Dayton Mitchell.)



In the past, stolen or counterfeited badges posed a threat, but using biometric information provides instant access to an indisputable identification. Guards at U.S. installations watch as individual workers insert their badge into a reader and simultaneously place their finger on a scanner. The badge, issued by the Biometric Identification System for Access (BISA), ensures that the person is the authorized worker. His/her identity is verified by comparing the fingerprint to one saved on the badge.

BISA is just one of many lifesaving biometric systems developed and deployed by Project Manager (PM) DOD Biometrics, part of Program Executive Office Enterprise Information Systems, an Army acquisition organization that

contributes technology tools for a wide range of defense warfighting, communications, and business missions.

### **Biometrics Systems**

The DOD-Automated Biometric Identification System Version 1.0 (ABIS v1.0) database supports *Operations Enduring* and *Iraqi Freedom* by providing a central, authoritative repository for biometric records. It catalogues biometric data taken from detainees, enemy combatants, and other non-U.S. persons of interest. The prototype system was put into operation at the end of 2004, with the current ABIS v1.0 deployed in early 2009. ABIS v1.0 far surpasses the original prototype ABIS in both reaction time and capability. While

the original database stored and matched fingerprints only, v1.0 adds capabilities for facial images, palm prints, and iris patterns, as well as fingerprints for adversary and neutral, unknown, or non-aligned population groups.

The new ABIS uses an advanced algorithm that combines partial matches of multiple biometric modalities and increases the ability of the system to supply a match without requiring human intervention, up to 28 times faster than the prototype. ABIS v1.0 accepts data from multiple collection devices and shares the information with other key U.S. military and intelligence systems.

Three PM DOD Biometrics systems are used to collect biometric data in Afghanistan and Iraq: Biometric Automated Toolset (BAT), Hand-Held Interagency Identity Detection Equipment (HIIDE), and BISA. BAT was developed in 1999 to deal with issues in the Balkans in which local nationals would cause problems on a U.S. installation, be removed, and barred from reentry, only to move to another installation and cause similar problems. U.S. officials did not have a system to establish and share history of individuals causing recurring problems on U.S. bases. Personnel at the Army's Battle Command Battle Laboratory, Fort Huachuca, AZ, responded with the BAT, a system consisting of a laptop computer with identification processing software and peripheral devices including a hand-held iris scanner, digital camera, and fingerprint reader. The laptops connect to a series of servers that ensure regular updates of vital biometric records. BAT collects and compares fingerprints, iris images, and facial photos used to enroll, identify, and track non-U.S. persons of interest to DOD.

The HIIDE, introduced in 2007, is a small hand-held, multimodal (iris, fingerprint, face) biometric collection and matching device. It is more portable than BAT, and it collects biometric, biographical, and contextual data on persons of interest and



PVT Marcus Lewis, 1st Platoon, Dog Co., 1/503rd Airborne Infantry, 173rd BCT, uses the HIIDE biometrics system to fingerprint a man in Wardak Province, Afghanistan, Feb. 2, 2010. (U.S. Army photo by SPC Deyonte Mosley.)

matches it against an internal database, downloaded directly from the BAT via a tether. The system visually indicates whether the identified person is on a watch list and can create tracking reports of biometric encounters for later intelligence analysis. It provides mobile identification solutions that enable Soldiers to identify and enroll subjects in the field quickly and accurately.

As mentioned earlier, BISA is a force protection device that collects multimodal biometric and biographical information to produce a biometrically enabled smartcard or personal identification number badge to manage access of U.S.-controlled facilities in Iraq. BISA incorporates fingerprint verification, iris matching, and palm print collection.

### Biometrics Example

In one example of biometric systems at work, a local national employee of a contractor company regularly comes through the base gates of an overseas

U.S. military facility, along with hundreds of others. Because he works on a U.S. installation, his fingerprints, iris, and photo images are recorded and sent to the ABIS v1.0 database in the United States. To gain access to the U.S. installation, he presents a biometrically enabled badge for base access, which is scanned by BISA, along with his fingerprint.

Months later, an Army patrol raids a suspected insurgent safe house. Family members are evacuated and Soldiers record their fingerprints, facial photos, and iris scans while other Soldiers search the house. Everything appears normal until investigators discover a hidden room with evidence of bomb-making activity. Everyone in the house is taken to a detention center where they are questioned and deny any knowledge of the hidden room.

The Soldiers confiscate everything in the hidden room and the forensics team discovers fingerprints on the bomb-making materials. Reports from DOD-ABIS indicate the fingerprints are from two people, one who was arrested during the raid. The bomb maker is separated from the rest of the household and detained. With the



PFC Logan Ayala takes in-processing "detainee" SPC Matthew Poore's image for the BAT system during training for Headquarters and Headquarters Co., 705th Military Police Internment and Resettlement (I/R) Battalion, at the I/R training facility, Fort Leavenworth, KS. (Photo by Prudence Siebert, Fort Leavenworth Lamp.)

bomber removed from their midst, the remaining family members tell Army interrogators about the two insurgents who used the room and threatened to kill them if they said anything. With the terrorist arrested, they now feel safe enough to cooperate with the U.S. military.

The match report from ABIS identifies the second set of fingerprints as belonging to a local civilian who works at a nearby U.S. facility, our local national contractor employee. The military remotely updates the base access system to alert guards the next time the man comes to work. The next day when our local national inserts his badge and scans his finger, guards discover that he is wanted for questioning, so they take his badge and detain him.

This vignette illustrates how biometrics can be used to apprehend insurgents tied to bomb-making activities. Just as importantly, it shows how biometric information can free innocent family members from the terror of hosting insurgents so they can go about their lives in peace. In our scenario, the fingerprint match occurred quickly enough for the bomb maker to be identified and brought into custody, limiting detention time of the innocent family members.

### Success

With these systems in place, insurgents have come to realize they can no longer gain easy access to U.S. facilities, and, subsequently, attacks have decreased. The key to their previous success was to remain hidden, often in plain sight, blending in with the local population. The American Soldier, unable to speak

Arabic and unfamiliar with the culture and customs of Iraq and Afghanistan, found it difficult to distinguish insurgents from the general populace. Biometrics has helped lift this veil of anonymity.

Having demonstrated their value, use of these biometric systems spread rapidly. At the end of 2009, more than 1,000 BATs and 7,000 HIIDEs were in use by the Army and the U.S. Marine Corps (USMC) in Iraq and Afghanistan, and biometric technology is widely credited with contributing to the U.S. military's success in Iraq. For example, after the much-publicized USMC operation to capture the Iraqi town of Fallujah, biometrically enabled identification badges were issued to the local population to ensure insurgents would have difficulty reestablishing themselves in the city. In 2007 and 2008, more than 1,700 matches linked individuals to improvised explosive devices in Iraq alone. The use of biometrics clearly had a positive effect on the overall effort.

This success led the Association for Enterprise Information to award the 2009 Excellence in Enterprise Integration Award to DOD-ABIS v1.0, saying, "This team of government and industry partners has given the warfighter a stronger, more reliable, and more effective tool that reduces the enemy's ability to hide among innocent civilian populations—and a tool that



The fingerprint scanner is one of three recognition tools the BAT system uses to identify an individual. (USMC photo by LCpl Thomas Provost.)

lays the foundation of a true enduring capability for DOD and its forces.”

PM DOD Biometrics provides tools that enable the U.S. military to effectively establish the identity of people they encounter during military operations. As situations demanded, the PM worked quickly to deploy effective biometric devices that enhanced identity management. DOD ABIS v1.0, BAT, BISA, and HIIDE expose insurgents and remove their ability to hide in local civilian populations, enhancing safety of Soldiers and the quality of everyday life for the people of Iraq and Afghanistan.

**JODY KIEFFER** is a technical writer and editor for PM DOD Biometrics. She holds an A.A.S. in data processing technology from Northern Virginia Community College and a bachelor's from the University of Missouri's School of Journalism.

**KEVIN TRISSELL** is a senior contract consultant to PM DOD Biometrics. A retired USAF officer, he holds a B.S. in physics and a B.A. in French from Oklahoma State University, a B.S. in meteorology from Florida State University, and an M.B.A. and an M.P.A. from the City University of Seattle, WA.

With these systems in place, insurgents have come to realize they can no longer gain easy access to U.S. facilities, and, subsequently, attacks have decreased.