

U.S. Creates Enemy Biometric Database

By JASON SHERMAN

The Pentagon has launched a pilot program to collect the fingerprints – and eventually DNA samples, palm prints, voice sounds and iris patterns – of potential enemies in its war on terrorism.

U.S. troops already are collecting fingerprints to feed a new military database that will be modeled on - and linked to - the FBI's fingerprint library, which contains the prints and criminal history of 47 million people and is the world's largest biometric collection. The prints are the first step in building what proponents hope eventually will be a comprehensive system that uses biometric factors to identify people.

Those being fingerprinted will include detainees, enemy prisoners of war, civilian internees and foreigners under U.S. government control who are perceived as national security threats and deemed to require further background checks.

“In the global war on terrorism, the Defense Department and the U.S. government cannot trust the names and documents that are presented to authorities in order to establish true identity,” John Woodward, director of the Defense Department's Biometric Management Office that is overseeing the effort, said in an e-mail response to questions. “We must develop a method for linking an individual to their past alias identities and activities, particularly criminal and terrorist activities.”

Lockheed Martin Information Systems, Seabrook, Md., which built the FBI's fingerprint system, was awarded \$5 million by the Pentagon on Sept. 10 for the first year of a five-year contract to begin building the military's fingerprint system.

Company officials issued a statement announcing the contract, but declined requests for an interview through a spokesman because of the “sensitivity of the project.”

Barry Steinhardt, director of the American Civil Liberties Union's technology and liberty program, said the Pentagon's biometric efforts are worthwhile – as long as they focus outward.

“What would worry me about this is that systems used by the Defense Department off American soil are going to find themselves migrating back to the U.S. and turned on American residents,” Steinhardt said.

Wider Sharing of Information

The Pentagon's new Automated Biometric Identification System and its databases will be based in West Virginia, near the FBI's Criminal Justice Information Services Division and Automated Fingerprint Identification System in Clarksburg.

The Biometric Management Office is spearheading a number of efforts to lay the groundwork to ensure biometric technologies are effective tools for the military.

The office is working to set standards that will permit U.S. government agencies to share and compare biometric data. And technical architectures are being crafted to organize how information will be stored, searched, matched and shared.

In February, the Pentagon's chief information officer required all military units that collect electronic fingerprints from "red forces" – a military euphemism for established or potential enemies – to comply with internationally accepted fingerprint standards.

In July, Paul McHale, assistant secretary of defense for homeland defense, allowed the military to match fingerprints from Iraq, Afghanistan and elsewhere overseas against the FBI's fingerprint database.

U.S. forces are now using the Biometric Automated Toolset, which was initially fielded to identify people brought to military detention centers. But about 80 percent of the prints collected with this system did not comply with international standards, and so could not be matched to the FBI's database. The new standards set in February and better fingerprinting devices will help, Woodward said.

New Biometric Frontiers

Fingerprints are considered the best available biometric tools, largely because of their wide use by law enforcement.

But facial and iris recognition soon may gain wider use, said Joseph Kim, associate director of consulting at the International Biometric Group in New York, which does work for the Department of Homeland Security and other federal clients.

"The technology is good enough to be a tool that allows you to do what nothing else really can," said Kim. "Nothing else can really replace biometrics to identify or verify people with something they always have."

Kim's group expects the market for biometric technologies to boom from the \$719 million notched last year to \$4.6 billion by 2008.

A Pentagon advisory panel to Defense Secretary Donald Rumsfeld recently recommended the military create a major program to link biometrics with new ways of tracking individuals to win the war on terrorism.

The Department of Homeland Security began using biometrics this summer under the US-VISIT program. Visa applicants must submit fingerprints and facial photographs, which are used to check identity when they attempt to enter the United States.