Military, Private Sector Rush to Adopt High-Tech Security Technology
David McGuire, washingtonpostcom Staff Writer

09/24/2002
Newsbytes News Network

United States, 2002 Sep 24 (NB). Deep in the Pentagon, an Army officer approaches a gray box affixed at roughly eye-level beside a wooden office door. The officer stares at the box, training his eye on a circular mirror about the size of a half-dollar. "Identification is completed," purrs a computerized female voice as the lock clicks, permitting the officer to pass.

The slick plastic box, a device that scans iris patterns and compares them to a database of iris images taken from personnel who are cleared for entrance, is just one of a widening array of products designed to identify individuals by their unique physical characteristics.

Such technology hardly seems out of place in the heart of America's military industrial complex. But after the Sept. 11, 2001, terrorist attacks, the iris-scanning device and other security technologies that focus on physical characteristics are cropping up more and more in civilian life -- at office complexes, grocery stores, schools and fitness centers across the country.

The science underpinning such devices is "**biometrics**," a field long mired in controversy, but one that has enjoyed a makeover during the past year.

Unlike access cards, the body parts that **biometrics** devices read cannot be easily lost, sold or traded among conspirators, and unlike security codes, they can't be forgotten. The appeal of such a reliable identifier has grown in the post-Sept. 11 environment, but the use of **biometrics** for security purposes has raised questions about potential privacy intrusions and whether the technology is sufficiently reliable.

Squatting across the road from a tiny regional airport in rural West Virginia, the U.S. Army's **Biometric** Fusion Center isn't the gleaming testament to scientific advancement one might expect. The building -- a smallish, low-slung structure of textured concrete and faded brown siding - offers few clues that it's the setting for leading-edge research into advanced **biometrics** technologies.

Past the outer door, however, the center starts to hint at its purpose. Barring entry to the main floor is an iris scanner identical to ones recently installed in the Pentagon.

Director Paul Howe said the iris scanner, one of several **biometric** devices in use throughout the building, serves two purposes: securing the facility, and giving staffers an opportunity to experience daily life with the device before recommending it for use throughout the military.

A device that is effective but annoying isn't an ideal solution, Howe said. "Part of it is saying, 'If I had to use it, would I really like it?'"

The Bridgeport, W.Va., center was founded in 2000 by the Army's then-fledgling **Biometric** Management Office (BMO), which is charged with spurring the deployment of **biometric** security devices throughout the military. The center has since become the testing ground for all

commercial **biometric** products considered for use by the U.S. armed forces.

Howe said Bridgeport was a logical choice to serve as home to the **Biometric** Fusion Center. In 2000, West Virginia University boasted one of the nation's few academic **biometrics** programs, and the nearby town of Clarksburg is home to the FBI's massive fingerprint database.

Center officials signed the lease on the dowdy two-story property in August 2000, and eventually engaged a staff of more than 30 contractors, working under the management of Howe, a civilian employee of the Defense Department.

Since its launch, the center has reviewed about 50 devices, clearing about a dozen for use in military applications, Howe said. "This is kind of a new industry. What we like to focus on are those very mature products that might be useful right away."

On the top floor, a small laboratory is strewn with tens of thousands of dollars worth of commercial **biometric** devices. Tiny fingerprint identification cards that can be plugged into laptops share limited desk space with chunky hand scanners and slick iris cameras. Devices deemed not ready for prime time rest forgotten beside those already cleared for use in military installations and those still facing a battery of tests.

Some super-secure military facilities use custom-made **biometric** devices not available to the public (or, for that matter, to the staff of the **Biometric** Fusion Center), but many mid-level secure military facilities rely on commercially available **biometrics** to provide an "added layer of security," Howe said.

One of the most recent installations was the Pentagon Officers Athletic Club, where the management office has placed iris scanners at the entrance to the popular gym.

Managers there say that, beyond creating a simplified mechanism to allow entrance to the athletic club, the placement of the **biometric** device in such a central location will help familiarize military personnel with technology that is likely to become far more prevalent in their lives in the coming years. Fitness-conscious military personnel of all ranks and security-clearance levels pass through the athletic center, BMO Senior Analyst Margo English said.

Placing **biometric** devices in such high-traffic places will ultimately acclimate not just military personnel, but the general public to the devices, allowing most people to get comfortable with **biometrics**, Howe predicted. "You're always going to have some people who find it awkward, just as my mother finds it awkward to remember a password," Howe said. **Biometric** devices perform one of two basic functions: verifying a person's identity ("authentication") and picking subjects/suspects out of a crowd ("identification").

Authentication devices -- including finger, iris and hand scanners -- are used to confirm the identities of people who have clearance to enter secure areas, log onto sensitive computers, or perform any other sort of restricted function. By contrast, identification technologies like face scanners take a more scattershot approach, picking subjects out of crowds by spotting their unique physical characteristics. Although a less commonly known application, face scanners can also be used for more traditional authentication purposes.

Biometric devices may come in many flavors, but all of them share the underlying recipe for

recording and comparing physical characteristics.

Whether scanning fingerprints, facial ridges, iris patterns or hand contours, all modern **biometric** devices first obtain "samples" by recording unique points on a target body part.

The samples are then converted to digital templates, which can be compared and contrasted at varying speeds and accuracy based on the level of detail included in the original samples and the thoroughness of the series of mathematical calculations (or "algorithms") programmed into the device that are used for processing comparisons.

Raj Nanavati, whose company International **Biometric** Group of New York tests devices for reliability, says the technology has gotten faster, smoother and more accurate in recent years. "The false rejection [and] false acceptance rates for finger, iris and hand are very low," he said.

Bill Voltmer, the president and chief executive of Moorestown, N.J.-based Iridian Technologies Inc., said iris scanners using Iridian's proprietary algorithm can reduce false acceptance rates (instances of unauthorized people being cleared for access) to almost zero.

But Voltmer conceded that the devices aren't completely foolproof, which highlights a recurring question about relying solely on **biometrics** to protect secure areas. The comparatively high reliability and seemingly tamperproof nature of the devices could lull users into a false sense of security, according to critics.

That danger was demonstrated earlier this year when a team of Japanese scientists released findings of a study in which they used gelatin and other simple household products to create "**gummy** fingers" capable of fooling fingerprint scanners.

But proponents of **biometrics** say that the devices aren't intended to replace armed guards or manned security checkpoints. Rather, the devices should be used to replace access cards and memorized security codes, which they say are much easier to defeat than comparable **biometrics**.

"Most of the access control systems today verify authorized pieces of plastic, when what they really want to do is verify authorized people," Recognition Systems Inc. spokesman Bill Spence said. Recognition Systems, a Campbell, Calif.-based unit of Ingersoll-Rand, is the world's largest developer of hand geometry scanners.

Richard M. Smith, a private Internet security consultant based in Cambridge, Mass., said **biometric** companies still face a tough task in selling their products to the public.

"These systems can do a good job of doing access control," Smith said. "The trouble is that they compete with other technologies like cards and key codes [that] tend to be less expensive and easier to deploy than a **biometric** solution."

Posting an anemic $20 million in sales in 1995, the **biometrics** industry will sell upwards of $200 million in devices this year, said International **Biometric** Industry Association (IBIA) Executive Director Richard Norton, citing IBIA sales projections. The **biometrics** industry posted sales of $170 million in 2001, and IBIA predicts annual industry sales of $2 billion by 2006.

Hand, finger, face and iris scanners account for most of the **biometrics** products sold, but companies are in the process of developing technologies to identify people based on their voice patterns, body heat signatures and keyboard-use characteristics, Norton said.

Biometrics companies say that the private sector is only a few steps behind the military in adopting **biometric** technologies.

The sector is small by most standards and has felt the pinch of shrinking corporate information-technology budgets, but many **biometrics** companies continue to post growing sales despite a languishing economy. And beyond the fiscal evidence of the industry's growth over the past few years, **biometrics** executives say the post-Sept. 11 security concerns have created unprecedented interest in their products.

"The direct impact [of the terrorist attacks] was the realization that crime and terror is actually a reality in our country and they pose a threat. It's a wake-up call," said Joseph Atick, president and chief executive of Identix Inc., a Minnetonka, Minn.-based firm that is one of the largest in the **biometrics** sector. "The wake-up call as a result of the shock of Sept. 11 has led people to accept any identification technology, within reason of course." Increased acceptance is critical for Identix, which deals in perhaps the most controversial breed of **biometrics**: face recognition. Critics of face scanners call the technology unreliable, questioning the ability of modern **biometrics** to accurately pick people out of crowds.

Biometrics "are very good authentication tools. They are terrible identification tools," said Bruce Schneier, president of Cupertino, Calif.-based Counterpane Internet Security and author of the monthly security newsletter, "Crypto-Gram."

"Where the industry is really overreaching is where they say, 'We can pick terrorists out of crowds,'" Schneier said.

"One-to-one" **biometrics** devices -- like the Pentagon iris scanners -- have a more proven track record, according to industry observers. Facing few roadblocks and riding a wave of heightened security concerns, manufacturers of those technologies are looking to ramp up deployment.

Schneier cautioned against over-reliance on the devices. "There are many circumstances in which **biometrics** aren't appropriate. That doesn't mean they're bad ... it just means they aren't the right tool," he said.

Howe, of the Army's **biometrics** center in West Virginia, said that use of the devices will continue to proliferate.

"They are getting slicker. They are getting less intrusive," Howe said. "They'll be as ubiquitous as credit cards."

Tomorrow: Civil liberties groups warn that **biometric** security devices pose serious threats to privacy rights.

Reported By TechNews.com, http://www.TechNews.com