

Charleston Daily Mail – January 9

“Distance Identification on Way, Official Says - Biometrics will Improve Some Security Measures”

George Hohmann

The head of the Department of Defense's Biometrics Management Office said identification technology is moving from the use of methods that employ direct contact, such as fingerprints and hand geometry, to methods that will identify individuals from a distance.

John Woodward said the goal of his office and its Bridgeport-based affiliate, the Biometric Fusion Center, is "to do all we can to make war fighters more secure."

For that to work, "you want to identify from a distance so you have time to react - call the guards, fire a missile, put up a barrier," Woodward said.

"We're not there yet," he added as he spoke to a large lunch crowd at the Alan B. Mollohan Innovation Center in Fairmont Wednesday.

He said the ability to identify individuals from a distance will probably involve a variety of technologies working together. Those technologies might include iris scans, facial recognition systems, odors, speech recognition systems and an analysis of a person's gait, for example.

Current security systems for facilities typically require the presentation of identification to gain passage through a gate. Once on the grounds of a facility, an individual is usually required to present identification to gain entrance to a building, must do so again to gain entrance to a particular room and, finally, must have a valid username and password to log onto a computer workstation.

"These systems don't talk to each other well," Woodward said. "Ideally, you want them all tied together."

Biometrics is the modern word for the science of linking physical characteristics to identity. "It's a high-tech word for an old concept," Woodward said.

The positive identification of individuals wasn't much of an issue prior to 1869 because, until then, the penalty for committing a heinous crime often was death. That meant governments didn't have to worry much about repeat offenders, Woodward said.

Efforts by government to tailor punishment to fit the crime gave rise to the need for identification - to link a person with his or her past acts, he said. Authorities originally used sketches and photos and went to jails to observe suspects.

By 1880, the most popular way to identify a person was to measure physical attributes and record peculiar marks. That didn't work well because it required trained people and special equipment, Woodward said.

Fingerprints quickly emerged as the primary way to identify individuals. In 1911 fingerprints were used to prove guilt in the United States and in 1924 the FBI became the steward of fingerprints in this country.

The FBI's computerized criminal master file, which became operational in 1999, allows the

agency to link a fingerprint to an individual in less than one hour, Woodward said. The FBI's Criminal Justice Information Services Division, which oversees the agency's fingerprint programs, is headquartered in Clarksburg.

Woodward said emerging identification technologies use medical, consumer, biographical, financial, biometric and behavioral information. "Biometrics plays a small but important role in data acquisition," he said.

Biometrics promises to increase security and convenience while decreasing costs. Biometrics also offers the capability to freeze or fix an identity, Woodward said.

That's a significant capability when one considers how difficult it is to prove an individual is who he says he is when that individual moves, presents false papers, uses aliases and lies, he said.

Positive identification has been especially troublesome on U.S. military bases abroad, which typically employ numerous foreign nationals, Woodward said.

By freezing or fixing an identity, authorities can make sure that for one felon there's one criminal record. "The FBI has mastered this," he said.

Fixing an identity also ensures that one foreigner applying for entry to the United States results in one U.S.-government travel document issued to the foreigner; one licensed driver equals one driver's license; and one soldier equals one identity, he said.

"We are looking at a technology that has a bright future," Woodward said. But he cautioned that every biometric benefit must be proven. "Help us document the case," he pleaded.

How it Works

John Woodward, head of the Department of Defense's Biometrics Management Office, said the identification process will involve numerous technologies including iris scans, facial and speech recognition, odors and an analysis of the person's gait.