

Inside the Army – September 29

“DoD Personnel Cite Cost, Reliability as Top Biometrics Concerns”

Anne Plummer

Cost and reliability topped concerns voiced by Defense Department personnel interviewed recently by the DoD Biometrics Management Office about fielding a department-wide biometrics capability, according to a senior program official.

Also high on the list is how to address policy issues, including privacy concerns, as well as employing biometric controls in the tactical realm, said John Woodward, BMO’s deputy director.

Biometric systems identify a person using a part of their body, such as the shape of their hand, fingerprint or iris pattern. Some military components already use the technology to safeguard access to computer systems or buildings. Pentagon leadership has tasked BMO, an Army-led joint program office, to coordinate requirements and acquire a single interoperable system, possibly using a central database to store biometric data collected from military personnel (Inside the Army, Sept. 15, p. 11).

Last June, RAND wrapped up a six-month survey of 54 DOD personnel on their perceptions of biometrics. Almost half of those interviewed represented midlevel personnel, with only 9.3 percent of those interviewed being political appointees. The majority of participants were located in the Washington area. While the final results have not been released, and participants are not considered an accurate representation of the entire military, several participants expressed interest in similar areas, Woodward said.

“Cost. Cost. Cost,” he told an industry audience at the 2003 Biometrics Consortium conference.

Of primary concern is finding the dollars to support and maintain a biometric system after it is installed, he said. Other priorities for warfighters include ensuring the system is efficient and robust enough to work in different environments.

BMO is still in the very early stages of determining how it will move forward with fielding an enterprise system. So far, the office has drafted an “initial capabilities document,” outlining in broad terms where the program is headed. The Joint Requirements Oversight Council and, eventually, the office of the assistant secretary of defense for networks and information integration will review the ICD to determine whether the program can begin concept and technology development.

In addition to finding a technical solution, BMO is also trying to address policy issues for biometrics. As mandated by law, the office is completing a “privacy impact assessment.”

While officials are primarily interested in acquiring a system that would help improve security for computers and buildings, biometrics in the tactical arena is on the horizon. Examples include adding a fingerprint scanner to a ruggedized, battlefield laptop or even a weapon system.

But improving security in the field presents a slew of new challenges that will have to be addressed over time, Woodward said. Among the warfighters interviewed by RAND, the issue of tactical biometrics was one of the “more controversial” topics associated with the new technology, he said.

“The tactical arena [is] very messy” and lends itself to complications, Woodward said. One example is the use of chemical and biological protection suits. If protective masks or gloves are worn, a fingerprint system will probably not work, he said.