

News Release

FOR IMMEDIATE RELEASE

Scott Sadlon, BRTRC/DoD BMO

Phone: (703) 253-0944

E-Mail: ssadlon@brtrc.com

Margaret McBride, U.S. Army CIO/G-6

Phone: (703) 693-3069

Email: Margaret.mcbride@us.army.mil

First of Five Biometric Protection Profiles Certified

Protection Profiles Pave Way for DoD Standards for Biometric Devices

WASHINGTON, D.C., February 23, 2004 – The Department of Defense (DoD) Biometrics Management Office (BMO) announced that the National Information Assurance Partnership (NIAP) has certified the first of five planned Biometric Protection Profiles for DoD and other U.S. Government agencies. Known as the *U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments*, this biometric protection profile specifies the minimum functional and assurance security requirements for biometric products operating in verification mode in medium robustness security environments. This Biometric Protection Profile Working Group, created and chaired by the BMO and composed of representatives from the National Security Agency, NIAP, U.S. Navy, U.S. Air Force, and other stakeholder groups, developed this biometric protection profile.

Biometric systems use technologies that positively identify an individual based on his/her measurable physical features or traits. This biometric protection profile applies to biometric systems that verify that an individual is he/she claims to be. In general, a protection profile establishes the minimum acceptable information assurance criteria for a given class of product, thus ensuring that agencies do not procure and implement devices that create a security risk to the U.S. Government's facilities and information networks. If a product fails to meet the protection profile criteria, National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 prohibits federal agencies from procuring that product for use on U.S. Government networks for logical or physical access.

This biometric protection profile establishes an objective benchmark for evaluating certain classes of biometric products for DoD and U.S. Government use. If a product meets the benchmark information assurance criteria, the product can be approved for acquisition. If a product fails to meet the benchmark criteria, it may be considered a security risk and not viable for use on U.S. Government networks per the NSTISSP No. 11.

###

The Department of Defense Biometrics Management Office is the central entity within DoD responsible for leading, consolidating, and coordinating the development, adoption, and institutionalization of biometric technologies for Combatant Commands, Services, and Agencies, to support the warfighter and enhance Joint Service interoperability. The Secretary of the Army is the DoD's Executive Agent for developing and implementing biometrics technology.