



BIOMETRICS

DEPARTMENT OF DEFENSE

www.biometrics.dod.mil

About DoD Biometrics

In wartime, the DoD's dependence on information as a tactical and strategic asset requires DoD to carefully control its networks and information systems. This need for access control is also critical at the special operations and weapon system level, where, for example, a U.S. military operative deep in enemy territory must quickly and securely communicate actionable intelligence back to other units.

Access control issues are important to the peacetime DoD because improving the efficiency of operations, including controlling access to installations, facilities, computer systems, and networks, depends on fast and accurate identification. DoD also operates a vast set of human resource services involving health care, retiree and dependent benefits, and troop support services. These services create the need for identity assurance to prevent fraud and abuse.

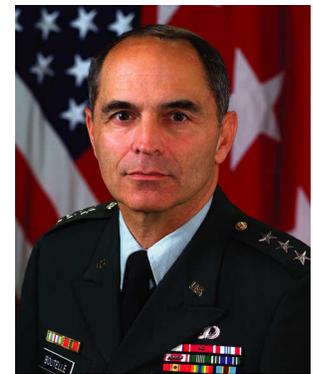
Congress, the White House, and DoD leadership recognize that biometrics, or automated recognition of a person using distinguishing traits, can be an enabling technology to provide better security through identity assurance.

Biometric systems take identity assurance beyond the basic "something you have" (e.g., token, badge) and "something you know" (e.g., user name, password), to "something you are" - a biometric. Biometric-based identity assurance systems rely upon physical or behavioral characteristics, such as fingerprints, hand geometry, iris patterns, etc., which are distinctive to individuals and can be measured to ensure that a person's identity is accurately determined.

The association between an individual and a "trusted identity" is the foundation for identity protection and management. A trusted identity is something that proves beyond a doubt that you are who you say you are (your identity has been "vetted") and that another person cannot "assume" your identity or masquerade as you (your identity has been "fixed"). Identity management is the process that creates and maintains the use of trusted identity.

With the vetting and fixing of a trusted identity, identity management can be further associated with a set of assigned permissions and access rights. Prior to the Information Age, DoD faced its greatest identity challenge in the area of physical access control. However, the exponential growth and use of information technology throughout the DoD has dramatically increased the security challenge for logical access control of which trusted identity is essential. Moreover, DoD must make better and more extensive use of biometric technologies as part of U.S. efforts in the Global War on Terrorism.

No one is more aware of this challenge than Army Chief Information Officer (CIO) LTG Steven Boutelle. The Secretary of the Army is the Executive Agent for biometric technologies in DoD and the oversight responsibility rests with the Army CIO. Borrowing from the Army theme, LTG Boutelle seeks to make biometrics "ready and relevant" for the DoD. He emphasized his guidance in his presentation to the September 2003 Biometric Consortium Conference: "Introducing biometric technologies into the DoD is not enough - they must be part of an integrated, interoperable, DoD-wide enterprise solution, in coordination with other U.S. Government initiatives."



LTG Boutelle has made it clear that standards development work should be one of the Biometrics Management Office's highest priorities. Without comprehensive standards in place, DoD runs the risks of creating insular, fragmented, and expensive biometric "fiefdoms" that will not be able to share data or communicate with one another. Such an approach is bad for the DoD and a detriment to national security.

Reprinted from April/June 2004 issue



September 2004