ARROYO CENTER

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore RAND Arroyo Center

View document details

How do you know friend from foe?

DoD's Automated Biometric Identification System

By John D Woodward Jr, Director, Biometrics Management Office, Department of Defense

In the global war on terrorism, the United States is pitted against a highly mobile enemy that attempts to disguise the identities and allegiances of its fighters. In a war without borders, uniforms or defined lines of battle, knowing who is an enemy is essential. As a result, the Department of Defense is striving to give our military forces – those deployed to faraway places and those standing watch on the home front – identity dominance, the ability to separate friend from foe by linking a person to a previously used identity or a past terrorist or criminal act.

To accomplish this task, US forces must be able to find reliable answers to key questions. For example, has a person who has been detained at a desert guard post or discovered on a suspicious ocean-going craft been previously arrested in the US or elsewhere? Has the individual used alias identities or fraudulent documents? Has the person ever been denied entry into this country? Has the person been linked to terrorist groups or attacks?

Stated names and supposedly 'official' documents by themselves cannot provide those answers reliably. Consequently, DoD, working with other federal agencies, is moving to give our warfighters rapid access to relevant databases of information based on biometrics – the measurable physical characteristics or behavioral traits distinctive to an individual.

The Automated Biometric Identification System (ABIS) initiative is a high priority of DoD's Biometrics Management Office and the Biometrics Fusion Center, the department's technical and operational center for biometric technologies. With the DoD ABIS, biometric data (with an initial focus on fingerprints) gathered by our forces from 'red force' personnel – detainees, internees, enemy prisoners of war and foreign persons of interest as national security threats – can be compared with data maintained by the FBI's integrated automated fingerprint identification system (IAFIS), an electronic, searchable database with the fingerprints of approximately 48 million people who have been arrested in the US. Databases of US government agencies will also eventually be linked so that red force biometric data is searched against multiple databases for any possible matches.

As the DoD Chief Information Officer explained earlier this year: "In fighting the global war on terrorism, standardization and interoperability are key tenants of success. And the department cannot afford to operate systems that do not fully communicate and share fingerprint data on 'red force' personnel with other US government systems."

On September 23, 2004, the DoD Biometrics Management Office awarded Lockheed Martin Corporation a five-year contract to design, build and maintain the DoD ABIS. The DoD Biometrics Fusion Center, located in West Virginia, will manage the DoD ABIS and ensure that it is fully interoperable with the FBI's IAFIS.

Although not a perfect solution, the DoD ABIS will be a powerful tool, providing US warfighters with timely and reliable responses to whether they face a friend or foe. After taking 10 rolled fingerprints in a procedure that meets recognized standards, trained military personnel will be able to submit the data to be searched against a wide array of pertinent databases. Answers to identity questions will be available in time for US warfighters to take appropriate action. For example, the discovery that an enemy combatant encountered by the US military on a foreign field had previously tried to enter the United States would be extremely significant. In this manner, the US government will be able to identify terrorists or other suspected national security threats. To illustrate, US officials matched the fingerprints of Mohamed al Kahtani, an enemy combatant in southwest Asia, to the fingerprints of a person who tried to enter the US on August 4, 2001. The 9/11 Commission concluded that this individual had intended to be the 20th hijacker during the September 11 terrorist attacks on the US.

DoD's biometric initiatives must continue to be forward looking and innovative. "At the end of the day, biometrics should actually get to the point where its use is seamless, interoperable, easy and instantaneous for the user," LTG Steven W Boutelle, the US Army CIO and DoD's executive agent for biometrics, explained. "In the context of the global war on terrorism, ultimately, it's all about information – accessing information and sharing information."

In the near-term, the DoD ABIS will be expanded to process and store biometric data such as face recognition. Positively identifying terrorists and potential national security risks is critically important to the global war on terrorism. Biometric technologies provide capabilities to meet the requirements of force protection, actionable intelligence and law enforcement. Appropriate use of these technologies will enable the US military to identify friend or foe, and will keep America and its allies safer. ∎

John D Woodward is Director of the DoD Biometrics Management Office.

"The department cannot afford to operate systems that do not fully communicate and share fingerprint data"