

Biometrics: defending the nation



IWA talks to Dr Joseph Guzman, Acting Director of the Department of Defense's Biometrics Management Office.

Recent international developments are accelerating the adoption of biometric technology for border entry and exit points, commercial security, access to secure facilities and networks around the world. As a result, a technology traditionally used in high-security government agencies and Sci-Fi films has been thrust into the public eye.

Dr Joseph Guzman is the Acting Director of the Department of Defense Biometrics Management Office (BMO). He serves the BMO by working to bring biometric technologies to the warfighters in the global war on terrorism, institutionalize biometrics throughout the department and coordinate with stakeholders within the Department and at the interagency level.

Having previously served as the BMO's Director for Policy, Planning and Liaison, Dr Guzman brings valuable experience in biometrics policy implementation and planning and in orchestrating relationships with key US government constituents, and he has a broad policy analysis portfolio in the areas of military manpower, privatization, national security, biometrics and education.

IWA. What role are biometric technologies playing in enabling the DoD (and for that matter, other federal departments and agencies) to better protect information, systems and networks?

JG. The DoD Biometrics Management Office provides technical expertise and advice when necessary regarding biometrics implementation and development. We also ensure that we have interoperable systems, and have published a standard for formatting and protocol of biometrics submitted to us.



DR JOSEPH GUZMAN

The obvious, more traditional role for biometrics is in their use for network access, but post-9/11 we've been more focused on the use of biometrics in providing physical access to facilities, and using biometrics to identify people coming in to contact with our facilities and personnel.

We're not currently exploring new ways to use biometrics for logical or network access; what we're looking at is expanding our capabilities into different modalities, and how to use these different modalities together.

IWA. What other modalities are you currently exploring, and how can these increase security?

JG. Well, we're enhancing the quality of the fingerprints we collect and are speeding up the time it takes to collect good fingerprints. Depending on the operating procedures involved, we're also collecting facial photographs and iris images; once we've put these different identifiers into a database and use them collectively, we'll have more than one way to identify someone – which will obviously improve security.

IWA. How are you coordinating with other government agencies and international standards bodies to establish appropriate standards, interoperability tools and testing frameworks for biometric technologies?

JG. I'm glad you asked about that. The DoD Biometrics Management Office has the lead activity for coordinating biometrics standards input coordination for the US government, through the National Science and Technology Council's subcommittee on biometrics. We also sit on the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to ensure the directions we're taking are compatible with international directions. As I mentioned before, we have also published the protocol standard that ensures that new submittals will be compatible with ours, and that our protocols are backwards compatible with those of the FBI.

IWA. And how much global coordination is there on these type of issues?

JG. It's substantial – we have an eye on the trends and are ensuring that we will be able to read other's files (and vice versa) as appropriate.

IWA. Homeland Security Presidential Directive 12 calls for a common identification standard for federal employees and contractors. What are the main obstacles to achieving such a target and what progress is being made in terms of meeting this directive??

JG. HSPD12 is a huge undertaking and represents a significant shift for the federal government. It's a very positive move and will require a lot of logistical coordination in terms of ensuring all the agencies have the capability to register and check biometrics at access points. We are coordinating with all these

agencies, especially with regard to the internal DoD activity, to make sure that what we set up is compatible with what others are setting up. It's largely a logistical challenge; the technical challenges are pretty much in hand.

We will not be fielding the systems themselves, but we are involved in making sure all the specifications are appropriate.

IWA. Of the myriad biometric technologies available, which would you single out as most applicable for DoD use?

JG. Up to now, we have focused on fingerprints because the value of having a biometric system in place increase proportionate to the size of the database you have available – and obviously, the largest databases are the fingerprint ones. As we build up the other databases, we'll begin to fuse that information and gain new orders of utility from them.

The next focus will most likely be on iris technology, but we're not closing any options at this point. We're constantly on the lookout for new technologies and new innovations.

IWA. How do you plan to integrate the various biometrics the Defense Department uses, make them interoperable and make it easy for biometric data to be collected and shared?

JG. The first part of this question is something we are doing already: increasing interoperability through the use of the proper protocols. A big emphasis of our work in this office is to ensure the information sharing architectures, both physical and virtual, are existent and operative and that's our focus going forward. We can make a lot of progress on the technology side, but if we're not sharing the data optimally we won't realize the value of our systems. Conversely, even with the existing technologies we can get a tremendous amount of increased value from proper and complete information sharing, both in DoD and throughout the government as a whole.

IWA. The repercussions of hacked or stolen biometric data could be enormous. How do you protect the privacy, integrity and authenticity of this data?

JG. There are information assurance requirements and measures in place, and we make sure that all of our activities are in accordance with those, and that they are in line with federal privacy policies, etc. I think that, ultimately, the value of having identities fixed is very high for all concerned; there are commercial reasons in addition to security reasons for having your identity assured. ■

BIOMETRIC DATA SUBMISSIONS GET AN UPGRADE

To be able to send to and read data from the Automated Biometric Identification System (ABIS), DoD Biometrics has developed a new specification that can be downloaded from its website. The DoD Electronic Biometric Transmission Specification (EBTS), version 1.1 and an overview of the system are available at the links below.

The DoD Electronic Biometric Transmission Specification (EBTS) augments the FBI Electronic Fingerprint Transmission Specification (EFTS) with DoD-specific transaction categories and protocols for enhanced functionality. While the EBTS is compatible with the EFTS and is based on internationally-accepted standards, the EBTS has been developed specifically with ABIS in mind and has extra features specifically designed for the DoD. The EBTS has been vetted through the Standard Working Group, the Army G-2, the Language Technology Office and several other organizations outside of the DoD, including NIST, DHS and FBI, according to Dr Ramy Guirguis, Chair of the DoD Biometric Standards Working Group.

For now, EFTS-compliant biometric submittals will remain fully compatible with the DoD ABIS. As technical specifications and standards are revised and as requests and recommendations arrive from the users new versions of EBTS will be released.