findBIOMETRICS.com interview of John Mears, IBIA Director

June 27, 2014

Peter O'Neill: The IBIA has been actively involved in providing information about U.S. exit and entry processing over the past several years. The IBIA has produced, and will soon publish, a new document that highlights some of the important areas that need to be considered moving forward. The IBIA information to be published is very thoughtful and relies on real world global deployments and offers several recommendations to help guide this process.

To give us a preview…can you tell us about the additional reasons for an exit system beyond visa overstays?

John Mears: Absolutely, Peter. Let's start with a bit of history. The first legal requirement for an entry/exit system dates back to 1996, when the focus was tracking foreigners entering and leaving the U.S., particularly to understand and control visa overstay situations. After the events of September 11, 2001, entry-exit tracking also became viewed as a national security issue. The 9/11 Commission strongly recommended that the country implement, as quickly as possible, a biometric entry-exit screening system including provisions for frequent travelers.   U.S. VISIT, using fingerprint biometrics in the already operating IDENT system, was established in 2004. It provides biometric identification services for entry to the U.S., but not exit at the present time.

In the years that U.S. VISIT and IDENT, now called DHS Office of Biometric Identity Management (OBIM), have existed, a number of beneficial uses beyond visa overstay estimation have evolved. The system is regularly used by a number of agencies in fulfillment of their missions, like: Customs and Border Protection; the National Protection and Programs Directorate; OBIM; the Coast Guard; Citizenship and Immigration Services; Immigration and Customs Enforcement; Transportation Security Administration, the Department of State, and the Department of Justice. The Department of Defense and the Intelligence Community interface and benefit from the system, as do 18,000 state, tribal and local law enforcement agencies around the country.

There is routine coordination on criminal matters. People who transit our borders sometimes are wanted criminals, terrorists, or on the watch list. The entry system helps in identifying individuals who have committed crimes, in uncovering the fraudulent use of lost or stolen or counterfeit credentials, and in identifying victims of crimes or disasters. These invaluable uses are all beyond the original mandate for just getting a handle on visa overstays.

IBIA has been told that on Entry, approximately 2,000 people a day are identified who have presented false identities and are identified by their biometrics. The Entry system also identifies about 6,800 people a day from the watch list. Certainly figures that give you pause. And this is just on entry or other non-exit operations.

There is little doubt that biometric exit checks at the border will be equally important. They will facilitate finding stolen or counterfeit passports, any outstanding wants or warrants that prevent a person from leaving the country, or if a person is a missing person that might be a victim of trafficking or other duress. Frankly, if I'm getting on a plane out of the country, I am most interested in things that may affect me after I've left our borders. I would like to know that my fellow passengers are who they say they are and that I don't have to be afraid of them or for them. There are certainly many lawful current entry applications that have evolved over time. I would expect that the same will be true for biometric exit processing. I can go on for a while, but Peter I think those are the salient points among others in the IBIA paper.

Peter O'Neill: John, I am always quite surprised to see outdated information in various reports that come across my desk. How as an industry, do we address some of these inaccuracies…for example, reports with erroneous statements about biometric accuracy? What are actual 2014 large-scale biometric true matching percentages for example?

John Mears: You may be referring to data from 2009 DHS exit pilots, which found lower accuracy rates than those documented in 2013 and 2014. Unfortunately, the older figures are widely quoted and then juxtaposed with other data, such as the citation that says present day *biographic* exit data from 2013 are 97% accurate. These two things are separated by at least 4 years in time and it is a bit of an apples and oranges comparison. If you look at the actual 2014 large scale biometric true match accuracies from DHS OBIM for IDENT, which is inclusive of all the applications that I talked about earlier for the IDENT types of data, it is actually a 99.8% true match rate in 2014. We also understand the 97% biographic accuracy rate refers to traffic with Canada, not global traffic as does IDENT. It is really important to get underneath the data. We need to make sure they are timely, and that they are actually comparable.

Peter O'Neill: I find it shocking to see old information like that still finding its way into new reports, but it is good that the IBIA is on top of these situations. What about things like speed claims in some of these reports that you read about?

John Mears: That is an interesting topic because it revolves around a couple of things. One is the public learning curve on the uses of these systems once they go into operation. If you are like me, a change at the airport security lane it slows us down a little until we learn the

routine. Then we kind of just do it without thinking about it. So there is some learning curve associated with it and that is only natural.

However, it is not accurate that biometric processing must slow the airline boarding process once the learning curve is overcome. For example, the take-up of kiosks and automated border control systems and e-gates around the world has actually shown that the processing times including local one-to-one biometrics matching are in the 10-18 seconds range for fixed installations. Current one-to-N biometric searches for the IDENT watch list take less than 10 seconds, as does the comparable FBI RISC list search. The observations of the 2009 DHS pilots of 30 to 68 seconds per passenger, while dated now, were associated with hand-held or laptop jump kit equipment. Even with this primitive trial configuration, no statistically measurable impact to boarding times was observed since the biometric and biographic verifications were performed during normal passenger queuing times. The fact that airports and CBP type organizations around the world are adopting and installing automated processing systems with biometrics included shows the advantages – the passengers like it better, it's self-service, automated, private and fast. Authorities that administer these systems find they help them to leverage their scarce resources and reduce labor costs because fewer agents are required for passenger processing, compared to the number of agents required for attended manual processing of each passenger. This frees up agents to only deal with exceptions, which is what they should be doing. Freeing up airline personnel and systems by doing things like including automating boarding pass reading should make the systems even more attractive to this important stakeholder community.

Peter O'Neill: That is interesting John and I think that our information would support exactly that scenario. We've been reporting on the biometric industry for about 12 years and in about the last 5 years there have been so many large scale deployments put into place at airports, at border control, that the real world data is available and you don't need to guess about these claims anymore. But I think that unless you're involved in the industry or have access to folks who are involved in these deployments you are relying on old and very dated information. I think that might be the case in a lot of these new reports. What about cost claims and things like that?

John Mears: This is a tough issue. I have seen a number of cost claims, often associated with an unfounded assumption of the need for attended exit staffing. The IBIA has questioned that conclusion. Beside the question of automated versus manual processing, the underlying requirements are not made clear. It is not possible to do an estimate without knowing the requirements. In addition, it is based on old data. In the intervening years the industry has made significant improvements in cost, accuracy, automation, efficiency, and ease of use – a trend we've all seen and expect from high technology. IBIA believes it is

critical for DHS to transparently re-evaluate the 2008 impact assessment that employs actual publicly available definitive requirements and current costs.

Peter, the IBIA believes that a biometric exit system will provide significant benefits to our nation – indeed to all nations around the world who are adopting such systems. IBIA also believes that a "crawl-walk-run" approach, with phased rollouts of a biometric Exit across airport, maritime, and land ports, is prudent, as reflected in legislation proposed by the House Homeland Security Committee. This will provide the opportunity to analyze the experiences of the numerous European and Asian countries that are implementing Exit systems, to assess the infrastructure needs, particularly with respect to land borders, to undertake appropriate modeling and analysis, and to develop more extensive political cooperation with Canada and Mexico with respect to the land borders – one country's exit should be the other country's entrance.

Peter O'Neill: John, thank you so much for correcting the misperceptions about the exit and entry program. Thank goodness the IBIA is around to correct these very dated misunderstandings by using real world situations and real world information that is available now. Thank you again for taking the time to speak with us today.

John Mears: Thank you Peter, it is always a pleasure.

###