Biometric Borders Essential for Security

By: Janice Kephart

After 18 years and eight statutes, the U.S. border security system still awaits a biometric exit strategy for all departing foreign national travelers. The repercussions reverberate throughout the entire security community and affect our national security. Customers of foreign national entry-exit data are not just the immigration system, but also include the federal, state and local law enforcement as well as the intelligence community.

Some terrorist fingerprints, recovered from terrorist safe houses and renditions by our military, are included for access by border inspectors at ports of entry, but no biometric check or matching occurs for departing foreign nationals. That matters when the Islamic State is recruiting within the United States and recent FBI arrests are of those seeking to leave the United States, join the Islamic State and carry out terrorist attacks within the U.S. homeland.

What occurs today at exit is a, relatively, real-time check by airlines routed through the Department of Homeland Security (DHS) for biographic watch list checks, including the Transportation Security Administration’s (TSAs) Secure Flight. In an age where identity theft is the most costly crime and U.S. passports are a high commodity in the terrorist and criminal counterfeit document underworld, a biographic check without a biometric check add-on significantly stifles national security outbound. The fact is, we do not really know if people are who they say they are. This is verified by the U.S. Government Accountability Office (GAO) statistics showing the current system has left more than one million individuals unaccounted for in their whereabouts.

From a national security vantage point: if the FBI had forensic evidence that Tmarlan Tsarnaev had departed the United States to Chechnya for terrorist training, rather than a misspelled name missed on a manifest list, perhaps the FBI would have learned of the Boston Marathon bombing plotting in early 2013 and prevented the attack.

The DHS Office of Biometric Identity Management’s foreign national database currently provides a 10 fingerprint enrollment of foreign nationals first encountered, or verifies re-entry. Simultaneously, these prints are run against the FBI’s Next Generation Identification system for a criminal and terrorism check. INTERPOL notices of wanted criminals, various immigration databases as well as periodic add-ins of confirmed terrorist biometrics gathered in military theater are checked as well.

Yet of greatest concern is that these biometric capabilities, being developed elsewhere by our military and the FBI, are of limited use in keeping terrorists out of the United States since only fingerprints receive a biometric check at entry, and absolutely no check at exit. This limits what law enforcement and intelligence officials can know to keep our country safe. The bottom line is, without a biometric exit in place and an out of date biometric entry system, it is likely we will never know the actual number of people crossing our borders who are associated with terrorism.

On April 28, 2015, the Senate Homeland Security Committee Chairman Ron Johnson (R-WI) called former 9/11 Commission border counsel Janice Kephart to testify on the issue of the United States’ continued failure to implement an immigration biometric exit. A video of the hearing is here. The 30 page testimony focused on the following issues:

- why a biographic and biometric immigration exit is essential for safety, national security, facilitation of
travelers, immigration integrity (including helping solve the illegal overstay problem) and airport efficiency

• an in-depth look at the Islamic State’s strategy on infiltrating the west using fake identification and aliases

• a short history of the legislation and program development on biometric entry-exit to date

• a review of more than 30 countries’ entry/exit systems currently deployed around the world

It is in a terrorist’s job description to avoid detection. As the Islamic State expands its brand of terror and widens its net with its worldwide call for other terrorists to join them, there has been a rapid rise for fighters to use fake passports to get out of their home countries undetected, travel into Syria and, if they survive, back out undetected to their designated locations. Fake passports, aliases and bypassing border checkpoints are critical to success. Curtailing this travel is critical to stopping the rising spread of terror.

On March 28, 2015, the Islamic State published its “How to Survive in the West 2015” guide for new recruits and members. Divided into chapters, the English translation begins with a section on the importance of changing and maintaining different personas depending on the audience: “Changing your identity is important because you will come across different people in this struggle... Identity change is so important that everything about you – your: (Alias name, Physical look, Voice, Meeting places, and even phone number.) are different to your real ones. This makes it extremely difficult for intelligence agencies to know who you really are if you always take security precautions before every meeting. If you can find people who can fake ID cards, that would be even better (and this may be possible if you can have contact with people in the dark underworld).”

It is our military that has frontline access to gather terrorist biometrics in theater. It is our immigration system that has the responsibility of stopping their entry or knowing who has departed. Until the military shares at least some of its biometric data with DHS and the FBI—and DHS deploys a full biometric exit—the true needs of national security will not be met.

About the Author:
Janice Kephart is 9/11 Commission and Senate Judiciary counsel, CEO of the Secure Identity & Biometrics Association (SIBA) and North Americas Director, BORDERPOL.