In my last column, I started to discuss the REAL ID Act, which is currently back in the news because of a resurgence of strong opposition to its activation in 2008. <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/08/AR2007050801899.html> I mentioned that I choose to dismiss one class of objections altogether: the notion that because there are ways around the restrictions of the REAL ID Act, therefore it should be abandoned.

A much more serious objection to REAL ID as a security measure is rooted in how we use identification and authentication for security. Bruce Schneier has written clearly about this issue in an essay from the 2004-02-15 “Crypto-Gram” newsletter. <http://www.schneier.com/crypto-gram-0402.html#6> In “Identification and Security,” he makes the point that identification does not in itself tell us anything about the threat posed by an individual. Instead, an identifier allows authorities to compile profiles about individuals based on their recorded behavior – behavior that would be harder to compile without a unique, consistent identifier. Consider how much harder it is to track people who travel by bus and pay cash for their tickets than those who travel by air and use credit cards; but then ask yourself if travel patterns are sufficient to allow effective identification of terrorists.


If a suicide bomber is sitting beside you on your flight from Chicago to Tampa, I really don’t think that knowing that person’s name before or after the explosion makes very much difference – in the absence of specific intelligence about that specific person. Simply having employees of state departments of motor vehicles demand birth certificates, green cards, US passports or other acceptable documentary evidence of legitimate standing as legal residents of the USA tells us _NOTHING_ about the risks posed by any individual.

More in my third and last commentary on this problem next time.

* * *

Special discount for Network World Security Strategies readers: For a 10% discount on the upcoming INFOSEC Year in Review workshop <http://www.itpg.org/events_infosec.htm> in Marina Del Ray, CA on June 4-5, 2007, use code WNW07 when registering online or by phone.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msiia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.