INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

Implementing a Biometric US-VISIT Exit: Debunking Inaccuracies about Biometric Identification

During the discussion of an amendment that would require a biometric US-VISIT exit in comprehensive immigration reform legislation, opponents made a number of statements questioning the feasibility, reliability, accuracy and cost of the technology itself.

These statements were erroneous. Unfortunately, the likely impact of these perceptions is to retard the application of biometrics by the U.S. government to the detriment of national security and the benefits of the most effective means of identification available today. It is interesting that, at the same time its use in the U.S. is being questioned, the use of biometrics is expanding by leaps and bounds around the world.

As the debate continues on the merits of an amendment that would require a biometric US-VISIT exit (and other provisions in the bill such as employment verification), the purpose of this memo is to provide more accurate information about biometric identification that can be used to set the record straight and ensure a debate that relies on the most accurate and up-to-date information.

Statement 1: The technology is not reliable.
Fact: Biometric technology is both proven and accurate. Contrary to various statements (there was no data provided to prove the statements), the technology provides the most effective means of identification available, according to the National Institute of Standards and Technology (NIST), the body that develops technology standards for the government.

Biometric identification is not a new or unproven technology; it is accurate, reliable and proven. NIST has studied biometrics extensively for years as have numerous organizations worldwide. National and international standards have been in place for years. Its use is commonplace by government and the commercial and consumer sectors.

Statement 2: The 'photo tool' provided in the bill is a more reliable means of identification than biometric identification.
Fact: The 'photo tool' is not a more reliable means of identification. According to NIST (Federal Information Processing Standards Publication 201-2, section 6.3.1, Table 6-2), visual inspection and comparison provides little or no assurance of identity. The photo tool in the bill, which was touted as superior to biometric identification, relies on manual visual inspection and comparison of photos; it does not actually use the photos as a means of automated biometric identification (facial recognition).

Biometrics provides positive identity with a high degree of certainty and, at the same time, preserves privacy, according to NIST. No other means of identification can make that claim.

- Because biometrics are based on an individual's unique physical attributes, they prevent

imposters from claiming someone else's identity and, posing as that person, gain employment, collect benefits, board an airplane, gain access to personal data.

- Passwords, PINs, or other codes, also do not provide positive identity. PINs and passwords can be forgotten, lost, stolen, and shared with friends and family. A machine readable, fraud and tamper resistant card only authenticates the card and says nothing about the identity of the cardholder.
- It also is the most convenient, simple and democratic form of identity authentication. There are no language, gender, age, race, financial history, or literacy requirements for users; it is simply the presentation of the individual's biometric.

Statement 3: There are no large-scale successful government programs that use biometrics.
Fact: Biometrics are commonly and effectively used in large-scale projects in the US as well as globally.

- FBI Integrated Automated Fingerprint Identification System (IAFIS) that is the global standard for identification. There are more than 70 million subjects in the criminal master file of IAFIS, and our national law enforcement communities (and others) submit as many as 300,000 transactions to the system every day.
- FBI Next Generation Identification system (NGI) is the multi-modal upgrade to the IAFIS system, adding enhanced latent print capability, palm print capability, automated face recognition, and options for additional biometric modes such as iris recognition. The database capacities and transaction rates for NGI, currently in development, are multiples of the current IAFIS system.
- US-VISIT entry. The US-VISIT entry program basically tracks all people who enter into the country (other than those from visa waiver countries) by requiring them to submit fingerprints for national security background checks as a condition for receiving a visa. The fingerprints are checked against U.S. watch lists. If cleared, the visa is issued. When the visa holders enter the U.S., they must provide their fingerprints to the border agent who then matches them against the US-VISIT database and watch lists. If the fingerprints match those collected for the visa and there are no watch list alerts, they are admitted to the U.S. It has been extremely successful. Since its inception, US-VIST has processed over 150 million transactions and the response time for matching fingerprints at the U.S. border is about 8 seconds
- Department of Defense biometric common access cards (CAC) that all military personnel are required to carry at all times (per DoD Instruction 1000.13), and is used for physical and logical (e.g. computers and networks) access control around the world. There are over 3.5 million active CAC cards, and over 17 million have been issued over the life of the program. DoD has deployed an issuance infrastructure at over 1000 sites in more

than 27 countries around the world, and continues rolling out more than one million card readers and associated middleware.

- TSA Transportation Worker Identification Credential (TWIC), a post-9/11 initiative to clear and credential all of our nation's maritime port workers. This is a biometric smart card with over 2.4 million enrollments to-date. (This program has been subject to criticism, some fair and some unfair. The problems have largely been the result of the failure of antennas in about 1 million of the first cards issued, not with the biometric scanners. The cards and antennas have been fixed, the old cards are being flushed out of the system, and system operations have improved dramatically.)
- HSPD-12 Personal Identity Verification (PIV) mandated biometric-capable smart identification cards for all executive agency personnel. Approximately 4.3 million federal employees and 1.2 million contractors have been issued an HSPD-12 compliant PIV card.
- The Intelligence community relies on biometrics for their missions. There are classified programs which use biometrics extensively.
- The Government of India has embarked on an ambitious program to biometrically (finger, iris) enroll all of their citizens (~1.2 Billion), initially to ensure accurate dissemination of Government benefits, but ultimately as an enabler for secure commerce of all types. The program is called "Aadhaar" under the Unique Identification Authority of India (UIDAI). This is the most ambitious biometric identification program in the world, viewed by the very progressive Indian government as a secure enabler of societal progress and economic growth.

Statement 4: People can easily change fingerprints and iris but not the face.
Fact: Fingerprints and iris are substantially more reliable than the 'photo tool' as well as facial recognition. In fact, the easiest way to pass as an imposter is by cosmetic facial changes – hair style and color, glasses or no glasses, facial hair, prosthetics, cosmetic surgery, and many other techniques. These techniques cannot easily be detected visually by humans. People can develop virtual identities and change their appearance with ease. In addition, variations in pose, lighting, and expression are problematic when dealing with facial recognition. According to the FBI, facial recognition is far less reliable than fingerprints and iris recognition.

In addition, the biometrics industry has developed countermeasures for commonly used spoofing techniques for fingerprints and irises, largely centered on liveness detection. For fingerprint liveness detection, a variety of techniques are used, including detecting blood flow and galvanic skin response. For iris liveness (a counter to fake iris contact lenses), pupillary response over multiple images under varying lighting is used.

Statement 5: The visa document is tamper and fraud resistant and the photo on the card cannot be changed.

Fact: Biographical documents, absent biometrics, are susceptible to tampering and fraud. Documents are not difficult to come by, forging has become increasingly sophisticated, and documents in themselves only prove you are in possession of something, not really 'who' you are. Even a machine readable, fraud and tamper resistant card can be forged and only authenticates the card and says nothing about the identity of the cardholder. (This is to be distinguished from an electronically readable smart card with biometrics and other data embedded and encrypted in the card, which is highly effective).

Statement 6: Disney has substituted photos for fingerprint biometrics at its access gates on the theory that photos are just as effective as biometrics.
Fact: Disney has not substituted photos for biometrics at its access points. To the contrary, Disney continues to use biometrics at all access gates and, as noted in numerous recent media reports, is in the process of upgrading and expanding its use of fingerprint biometrics. Please also check the Disney website at www.disney.com.