ibia INTERNATIONAL
BIOMETRICS & IDENTIFICATION
ASSOCIATION

Source: International Biometrics & Identification Association
On Tuesday, May 20, 2015 at 12:01 AM ET

IBIA Says Expanding PreCheck Should be Based on Strong, Proven Security Standards

WASHINGTON, DC / ACCESSWIRE / May 20, 2015 / The International Biometrics & Identification Association (IBIA) strongly questions the Transportation Security Administration's (TSA) exclusive use of biographic data solutions in its prospective attempt to expand the PreCheck travel screening program. As TSA works on re-issuing its Request for Proposal (RFP), IBIA believes that biometrics should remain at the core of the PreCheck vetting procedure.

On December 23, 2014, TSA issued an RFP for PreCheck expansion that seeks third-party vendors to "pre-enroll" passengers into the program. TSA's proposal would authorize private vendors to use commercial data and proprietary algorithms to create a "risk-score" for passengers to determine eligibility.

Though the RFP was temporarily withdrawn for a series of technical and policy reasons that are currently being resolved, TSA has made clear its intention to change the established screening process for PreCheck applicants to rely on information from commercial data brokers and proprietary risk-scoring algorithms. As the RFP language is altered in anticipation of a future re-release, TSA has the opportunity to move in a direction that favors accurate matching against records of material value through biometrics.

According to Tovah LaDier, IBIA's managing director, "this new practice lacks the necessary accuracy to identify security risks and poses a serious threat to applicant privacy, noting that the current system of biometric-based FBI criminal history records checks (CHRC) has a true match rate on fingerprints of 98.6%, whereas the performance of these algorithms varies greatly and remains largely unproven on such a mass scale."

The FBI biometric-based CHRC is acknowledged as key to background checks worldwide as well as in the US. It has been the cornerstone of TSA's security threat assessment approach for the program. Now TSA proposes that vendors perform less-reliable, name-based background checks, as well as amass personal information from social media, location information, retail purchase history, and blog posts.

As Chris Calabrese, senior policy director at the Center for Democracy and Technology, told the FederalTimes, "We're talking about teaching machines how to spot dangerous behavior. It's easy to do when you're talking about credit card fraud; there's billions of transactions and lots of fraud and you can teach the machine exactly what to look for. It's very hard to do when it comes to terrorism, for which there are very few examples and which are very diverse."

Biometrics already lie at the heart of the traveler vetting performed by most DHS components - the benefits of which are widely known. TSA's sole reliance on biographic checks fails to take advantage of the significant record base and experience that DHS already has in identifying security risks.

In addition, TSA's proposed reliance on commercial data and proprietary risk-scoring algorithms also poses a serious threat to privacy. It is common knowledge that data on the Internet contains many inaccuracies. Personal biographic data, addresses, driver's license numbers, and credit card numbers that would be collected, have real value to cybercriminals and fraudsters and would leave private vendors vulnerable to hacks and incidents of identity theft.

This is not the case with biometrics in prescreening applications like PreCheck. A fingerprint or other biometric only describes one thing, a user's physical identity, and is of little value compared to large amounts of personal biographic, and other commercial data.

The IBIA urges the TSA to reconsider its plan to rely solely on private company partnerships aiming to use biographic data in the PreCheck application process. Any reasonable and secure prescreening program must include biometrics for background checks and identification reliability to maintain a high-level of accuracy in identifying security risks.

ABOUT IBIA.

IBIA advances the adoption and responsible use of technologies for managing human identity to enhance security, privacy, productivity, and convenience for individuals, organizations, and governments. To effectively carry out its mission, IBIA focuses on three core activities: Advocacy, Connections, Education. For more, please visit www.ibia.org.

Contact:

Tovah LaDier
Tel: (202) 587-4855