



1/10/2008 8:03 PM

Positional White Paper (Op-Ed) 01/08
(Jan 2008 - Vancouver, Canada: ACG-CIS) © 2008

US VISIT PROGRAM – A DOOR WITHOUT A LOCK?

A False Sense of Security Is More Dangerous Than No Security At All

(ACG-CIS) The US-VISIT program was created to provide some semblance of border security but it may be quietly failing as a useful tool to combat criminal activity entering the US. There are two perceived flaws that were discussed as early as 2003, one inherent and the other exploitable, in the design but they do not appear to have been properly addressed.

The solutions for these technical flaws in the fingerprint database are relatively simple, but to date there has been not one agency willing to implement the fix for them. Now, with the recent US announcement to move to scanning more fingerprints, the concern regarding these flaws is more pressing. The US-VISIT program intends to make increases to the front end of the system (fingerprint scanning locations and devices) while the backend (the database and the software processing it) is still weak.

P.T. Wright, Acting Deputy Director of US-VISIT, recently outlined U.S. plans to move from taking two digital finger scans to 10 finger scans from visitors to the United States. According to the official transcript of a press event held in the Consular Section of the U.S. Embassy to Brussels¹ June 25, 2007 Mr. Wright stated in part that

“..in January 2004, the US-VISIT program began capturing at all the airports and then subsequently our land border ports a two-print biometric capture of visitors to the United States from VWP [Visa Waiver Program] countries as well as from Visa countries.

One of the questions I’m often asked is why are we moving to a 10-print capture? Well, it’s pretty basic. Ten prints give you the full gallery of a person’s fingerprints. This will allow us to not only have greater security because we’ll be able to identify dangerous people beyond just the two prints; but also it allows us to begin facilitating individuals as our print galleries grow in size.

To date we almost have 100 million prints. As more people arrive and that grows –”

The US VISIT program was implemented as government sponsored screening process of persons wishing to enter the United States for travel and business. The original objectives were basic –

¹ *US-VISIT's Wright Explains U.S. Transition to 10-Fingerprint Collection at Borders* June 25, 2007
http://www.dhs.gov/xlibrary/assets/cfo_par2006_fullreport.pdf



know who is coming and in and use biometrics as a method for denying entry to those implicated in terror activities. In a post-911 world, this seemed to be a solution that would be workable now and well into the future.

However this security blanket, while having the appearance of providing security for US citizens, does have some central flaws. These flaws are based on the technical aspects of the program and after great discussion among those in the IT community were pointed out to the various levels of government responsible for the program. These discussions in 2003 and 2004 generally focused on the two perceived major flaws with the program. As predicted then, these flaws are now poised to become a very true reality that may compromise the system and render it relatively ineffectual.

These flaws have been obvious to those in the IT security community and to various persons knowledgeable with the technical underpinnings of this technology since 2003 - 2004. It can also be safely assumed that other IT persons elsewhere in the world know about these flaws through technical forums and their own general knowledge and training. It can also be further speculated that some of those foreign IT specialists may have ties or even work for organizations with negative interests towards the US. This information is not classified but it has not reached the general populace probably due to the fact that the average person may not fully understand or appreciate the technicalities involved. There may be other reasons why there has not been any open discussion regarding these technical flaws but those discussions are of a socio-political nature and are beyond the scope of this paper.

The first major problem is simple. It is the lack of a quick search capability due to the fingerprint database size and its exponential growth. Since January 2004, the US-VISIT program has collected over 100 million fingerprints from 50 million visitors. At one kilobyte of information per fingerprint², that is a database in excess of 100 Gigabytes. One Gigabyte of data could hold the contents of about 10 yards of books on a shelf whereas 100 Gigabytes could hold the entire library floor of academic journals.

If this same rate of growth is maintained, the US-VISIT program could conceivably have a database in excess of one Terabyte. A Terabyte³ is approximately one trillion bytes, or 1,000 Gigabytes. To put it in some perspective, a Terabyte could hold about 3.6 million 300 Kilobyte images or maybe about 300 hours of good quality video. A Terabyte could hold 1,000 copies of the Encyclopedia Britannica. Ten Terabytes could hold the printed collection of the Library of Congress. That's a lot of data and that represents only the fingerprint portion. Further identifiers are then added including pictures and relevant personal information creating a database of even larger proportions.

² from the Automatic Identification and Mobility (AIM) Technologies website – “Technology – Biometrics” ©2008

³ © 2008 What's a Byte - All rights reserved. From their website - *Megabytes, Gigabytes, Terabytes... What Are They?*



The US-VISIT program has announced that they are exploring the implementation of real-time online processing of visitors. There are currently multiple database access points for input and retrieval of the fingerprint data throughout the US and abroad. Now, according to Mr. Wright's statement, the US-VISIT program will start collecting 10 fingerprints per person in place of the current two. That increase of data collected will increase the size of the current database fivefold.

There are also plans to introduce real-time online processing of visitor fingerprints. Given current telecommunications and bandwidth limitations both in the US and abroad a full search could be hours if not days to complete. In land border crossing scenarios it is feasible that a complete search may be completed only after the visitor has entered the US. Current policy seems to echo this as the program verifies the visitor as having entered the US however the US-VISIT program can only report if the guest has overstayed after they have failed to biometrically check out within 90 days of arrival.

Current time estimates for search times are 10 seconds for a comparison to the 3.5 million names on the so-called Watch List; however US Consulates admit that a complete biometric database search requires a full business day before results are known. These response times are currently indicative of a database approaching critical mass where the time spent waiting for the search to be completed does not correspond to the usefulness of the search results in a timely manner.

There is current available database technology could help alleviate this problem. As an example, the B-One database (developed in Canada) can reduce search time by a factor of six. In other words, based upon current conditions, a 3 million item search can be completed in less than 1.5 seconds⁴.

The second problem is an exploitable flaw wherein the fingerprint records entered are based upon data from the weakest source, namely the enrollee. Simply stated, the fingerprint registered is linked to the identification presented but if that identification is wrong (or false) then the record is useless.

A person could enroll as John Smith and present their identification and offer a finger scan which links that fingerprint to that particular set of identification documents. However, if the person is not John Smith then those documents are wrong and who really is the person presenting the fingerprint for recording?

A brief explanation of the two styles of biometrics may help clear some of the mystery surrounding this technology.

AFIS Biometrics is an acronym for Automated Fingerprint Identification System. The finger scan is taken in the form of a digital image which is then processed by an algorithm to create a database record. This image can be from a live person, from a latent fingerprint taken from an object or

⁴ From the *B-One datasheet*, DPI International ©2008



any other type of process where the picture of a fingerprint can be captured. This image is linked to identification data and then is stored. This can be likened to the automation of the old stereotype of a person in the FBI basement sorting through fingerprints looking for a match. AFIS Biometrics is useful in situations such as criminology and forensic analysis. As AFIS Biometrics relies upon an image to be recorded, if the fingerprint was to be altered then the recorded image could be wrong (typically known as the 'gummy bear' or crazy glue' scenarios).

Applied Biometrics is used in applications such as door access, computer access and other situations requiring the activation of a mechanical or electrical device. The difference in the two technologies is that the fingerprint is "scanned" by a chip that records the image through the use of capacitance. Simply stated, the fingerprint is scanned by measuring the electrical capacitance in over 300 points on the finger. Altering the surface area of the fingerprint will not impede performance as the capacitance is measured below the surface skin layer into the epidermal layer where the fingerprint resides

Applied Biometrics technology requires the scan to be of live tissue only. It will not accept images of fingerprints nor those of fingers which have been cut off of a victim. In this sense, Applied Biometrics is better able to verify the user as it requires the actual registrant to both be present and alive.

The drawback to Applied Biometrics is that it cannot determine if a person has registered the same fingerprint more than once. But, once more, with the use of a more suitable database (again, the B1 database is such an example), this problem can be mitigated.

Therefore the crux of the second flaw is that the program cannot completely assure that the registrant is who they say they are and, in some instances, may allow the user to register more than once under multiple identities.

These problems were, as noted earlier, approached and discussed as early as 2003, before the US-VISIT program came into effect. Again, migrating to better suited database solutions with capabilities similar to the B-One database technology would be favourable in reducing the fallout from these potential flaws. In the same process this currently available database technology allows for the possibility to combine the record keeping of the AFIS biometrics with the authentication ideals of Applied Biometrics in both a fixed database and virtual online database configuration all while greatly decreasing search times and greatly increasing accuracy.

In 2005 the Center for Immigration Studies issued a multiple page report⁵ which offered, in part, as its conclusion

⁵ *Modernizing America's Welcome Mat - The Implementation of US-VISIT* August 2005 By Jessica M. Vaughan, Center for Immigration Studies



"When asked about the policy at a recent gathering, senior Customs and Border Protection (CBP) official Robert Jackstra spoke candidly: "The technology is there -- we can do it, but someone needs to make the decision to do it, and I don't see that happening. It is too politically sensitive." Representatives of numerous private companies who have been involved in border security contracting agree that the task of screening and logging 200 million visitors a year is feasible, and at least one company included the capability in its US-VISIT bid for work, but DHS has yet to express a commitment to that objective.

Need for Exit Recording

The exit recording component of US-VISIT was originally conceived as a way to monitor visa compliance patterns and reduce overstays and as an investigative tool to enable officials to determine if an individual of interest has departed the country. For now, DHS plans only a limited implementation of the exit program, to cover only regular non-immigrant visa visitors and visa waiver program visitors. Again, most Mexicans and Canadians visitors will be exempt.

Lack of attention to the overstay problem continues to compromise our efforts to prevent terrorist operations and control illegal immigration. At the moment, in a dangerous international environment, we are admitting about 200 million temporary visitors a year, with virtually no way to keep visitors from staying beyond their authorized visit, and no way even to count the number of visitors who overstay. DHS estimates that at least 30 percent of the approximately 10 million illegal immigrants living in the United States are probably visa overstayers. The Government Accountability Office (GAO) says that figure is almost certainly understated, probably significantly so.⁶

The current version of US-VISIT (and indications are that the current version is the administration's preferred final version) is incapable of assuring the integrity of the visitors and their documents in such a program. As noted above, since very few visitors using the land borders (which is likely to be the entry point for most people using a new guestworker program) are now checked, and those who are checked are routed to secondary inspections areas, there is no procedure or infrastructure in place, or planned, to enable immigration inspectors to authenticate the identity of large volumes of new land border crossers. Nor is it currently realistic with the existing infrastructure and staffing to run security checks for hundreds of thousands or possibly millions (depending on the program enacted) of new guestworkers, whether at the border, in the consulates, or in DHS district offices or service centers. Immigration officials have said privately that the background checks alone (outside of other processing procedures) for applicants to such a guestworker program would take several years to finish."

⁶ *Overstay Tracking is a Key Component of a Layered Defense*, Statement of Nancy R. Kingsbury, GAO report number GAO-04-170T.



In conclusion, the US-VISIT requirement of using 10 fingerprints will only ensure the accuracy of the enrolling documents presented. In addition, with the mandate to retain all records for 75 years from enrollment, the US-VISIT database is going to face challenges regarding access, search and manageability. The further problem of the exploitable flaw of wrong or false information being presented and accepted at the time of the fingerprint enrollment will only exacerbate the potential for problems, break downs and security breaches.

Unless this program is properly thought out and overhauled, unless this program utilizes technology currently available such as the B-One database engine or equivalent, the future of it's operation as an effective tool in combating criminality and terror is questionable. It will remain between the citizens of the US and their officials to determine the best course of action in these matters.