

## **US-VISIT Biometric Exit: Feasible and Low Cost Solution**

### **Overview**

Congress first mandated an automated entry-exit system in 1996 under the IIRIRA and amended the legislation to require the use of biometrics in the PATRIOT Act ([PL 107-56](#)) and the Border Security Act of 2002 ([PL 107-173](#)), passed in 2001 and 2002, respectively. The purpose was to collect a record of departure for every alien for matching against alien arrival records to allow identification through an online matching system.

Biometric entry has been operational since 2004. It started at 115 airports and 14 seaports in January 2004, expanded to the 50 busiest land ports of entry by the end of 2004, and has been operational at virtually all US ports of entry since December 2006.

In contrast, US-VISIT exit has not yet been implemented. To date, matching has been based on biographic data drawn from the I-94 documents issued to aliens. According to the February 2013 report by the Congressional Research Service (CRS) entitled *Issues in Homeland Security for the 113<sup>th</sup> Congress, page 47*, “...biographic matching (i.e., names, birthdates, and other identifying information) cannot confirm the identity of departing travelers”. CRS continues by noting that the “Collection of biometric data from exiting travelers would confirm their identity by matching fingerprints against ... the records in IDENT.”

In the decade since the inception of US-VISIT entry, it has been argued that a biometric exit is not feasible and also too costly. The International Biometrics & Identification Association (IBIA) and the identification technology industry in general take issue with these conclusions.

In summary, the identification technology industry is confident that it can implement an effective, reliable and efficient biometric exit program at U.S. airports that process international travelers, using proven and reliable off the shelf technologies and without disrupting airline operations and passenger travel. The industry also believes that the use of biometrics will provide the low cost solution to a mandatory exit program, at a cost that is significantly less than the exceedingly uncertain and dated \$3.5 billion cost estimate that has circulated (from “Air/Sea Biometric Exit Project”, April 17, 2008, DHS-2008-0039-002).

The International Biometrics & Identification Association (IBIA) is a non-profit trade group that advocates and promotes the responsible use of identification technologies for managing human identity in our digital world. The membership is comprised of global leaders who are involved in virtually all the major biometric government projects around the world as well as in the commercial and consumer mobile, financial, healthcare, and entertainment markets.

## Feasibility of Implementing US-VISIT Biometric Exit

For the following reasons that are discussed in detail below, the identification technology industry is confident that it is feasible to implement a biometric exit:

- This is not an untried program. Such systems are commonplace around the world.
- US-VISIT has been highly successful, providing a strong foundation for a biometric exit.
- Biometric exit leverages the biometric enrollment at US-VISIT entry.
- Biometric exit will be simpler and more efficient than other suggested solutions and will establish with a high degree of certainty that the person leaving the country is in fact the person who entered.

### Biometric entry/exit programs are commonplace around the world.

Biometric entry/exit systems are already successfully deployed around the world, including Amsterdam, France, the United Kingdom, and other countries in the European Union, Australia, New Zealand, Hong Kong, South Africa, Israel, Saudi Arabia, and UAE. These systems use a variety of biometrics (fingerprints, iris, face), depending on their specific needs. Many of the companies represented by this letter are involved in these projects and have the expertise and experience to implement a biometric exit in the U.S.

### Biometrics is already the cornerstone of U.S. immigration programs.

Biometrics are at the core of US-VISIT entry today. Under the current US-VISIT entry system, U.S. Government personnel take a digital photo and 10 fingerprints for all foreign nationals who enter the country at our international airports, including those who are required to obtain visas to enter the U.S. and those from visa waiver countries. For visa holders, these fingerprints are matched against the US-VISIT database and watch lists. If the fingerprints match those collected for the visa and there are no watch list alerts, and the individual does not exhibit behavior that requires further inquiry, they are admitted to the U.S. For visa waiver countries, the fingerprints are matched against the watch lists. If there are no hits, the person is admitted.

There are over 150 million fingerprints in the US-VISIT database and the search time per person is approximately 8-10 seconds. This database handles over 200K total transactions per day. This includes an average of 30,000 queries a day by the Departments of Defense, Justice and State; local and federal law enforcement; Interpol and intelligence agencies to verify identities for the purpose of immigration, law enforcement and national security.

As background, the National Institute of Science and Technology (NIST), the organization that sets technology standards for the government, analyzed the feasibility of US-VISIT in 2004 at the request of DHS and concluded it was feasible. Indeed it should be noted that NIST determined the system's feasibility at the outset. The exceptionally successful record of US-

VISIT in the past decade confirms NIST's conclusions.

The biometrics industry also has years of successful experience in large scale deployment at embassies and consular offices overseas where it is responsible for the intake of the digital photos and fingerprints that populate US-VISIT database today as well as at airports of entry.

In addition, other biometrics, such as face and iris, are available now and can be added to US-VISIT as the program expands to incorporate these so-called "stand-off" biometric technologies.

#### Biometric Capture and Document Authentication Technology - How it Works at Exit.

A biometric exit is technologically simpler than entry. After enrollment, the biometric search at entry requires searching against large-scale databases to identify whether a person is on a watch list. This requires 10 fingerprints and significant computational power.

In contrast, at exit, all that needs to be checked is whether the person leaving is the same person who entered the country through US-VISIT. There is no need to take another photograph, or to search the large watch list databases. This search can quickly be done using two (2) fingerprints to match against the fingerprints of the claimed identity already in the record in the database.

The process on exit will require the passenger to first submit a passport or other travel document. The document number will lead to the traveler's record in the US-VISIT database. Then the traveler submits the two (2) fingerprints. If there is a match with the fingerprints in the specific file, the individual will be cleared to exit, unless there are behavioral questions that would justify further screening.

#### Biometric exit will be simpler, more accurate, and more efficient than other proposed solutions.

Checking biometrics on departure is the most accurate way to know with a high degree of certainty who has exited the country and, in the most efficient way. All that is required is to match the fingerprints of the visitor with the existing database the entry system has developed.

Comparing photos and documents visually, attempting to match names, and asking a few secret personal questions are not as effective as biometrics as a means of identification. In its recent FIPS 201-2 publication, NIST concluded that visual inspection of credentials provides little or no confidence of identity, whereas adding biometrics provides a high degree of assurance of positive identity.

The proposal to use enhanced biographical data with 'secret personal' questions with no biometrics, does not provide identity with the high degree of certainty. Like Passwords, PINs, or other codes, the secret personal questions can easily be forgotten, lost, stolen, shared with

others, or sold. Also, much of this data is collected from the web, which is notoriously incorrect, and the source of information for identity thieves who build virtual identities that they then use or sell. With this approach, both privacy and security are at greater risk.

Moreover, it is quite difficult to see how visual comparisons and asking questions is more efficient than processing biometrics on departure. This kind of processing is labor intensive and slower than an automated biometric check.

#### Biometric Exit will not disrupt aviation operations or passenger travel.

While we appreciate the concerns noted by certain aviation stakeholders that the mandatory biometric exit might be disruptive to operations and passengers, the identification technology industry believes that an effective and secure biometric exit control system can be implemented without disrupting airport operations, or unnecessarily delaying travelers, and, further that a biometric exit can facilitate exit and reduce the burden on airline employees. Some of this push-back revolves around the concern that airline employees will be “conscripted” to do the Exit processing.

#### *DHS 2009 biometric pilot found no traveler delays*

The findings of the 2009 US-VISIT pilot program, predicated on the existing gate system, concludes there were no adverse effects on traveler line queues or inconvenience in making flights. Only foreign travelers are processed, which, depending on the airport and specific flight, is a variable fraction of total travelers.

#### *Processing of foreign passengers departing the U.S.*

Rather than use airline employees to process foreign travelers on exit, there are two options. One option, as provided in S. 744, is the use of Customs and Border Protection (CBP) personnel to staff the exit processing, as they do on entry, the cost of which would be covered by the government.

An alternative option is to use fully automated systems similar to e-Gate systems in use at airports in Europe, Asia, and Australia. This would significantly reduce the number of personnel required as one (1) border control agent can monitor multiple automated gates. An automated e-Gate installation might be used at the entrance to an international terminal (after the security checkpoint) or at a group of airport jetway gates.

#### **Cost Estimates of a Biometric Exit**

As representatives of the identification technology industry, we are confident about providing costs of the biometric component technologies that could be used in a biometric exit system.

However, that is not the case with overall system costs. Without an understanding of the system requirements and specific implementation objectives (e.g., which air, maritime, and land ports are involved), it would be irresponsible to attempt to estimate an overall cost.

The industry believes, however, a very robust, viable biometric system can be developed at significantly less than half of the estimated \$3.5 B proposed in the 2008 DHS study referenced earlier (which covered **73 airports and seven seaports for a period of 10 years**). The cost for a biometric exit at airports alone would bring the cost down even lower.

Although the analysis prepared in 2008 was based on the best available knowledge at the time, the report itself is quick to point out that it is only a Rough Order of Magnitude (ROM) estimate based on “lack of data concerning several variables in this analysis,” as a result of which the estimated costs are vastly overstated.

Most significantly, the 2008 study designated its cost estimate as a “Class 5” cost estimate as defined by the Association for the Advancement of Cost Engineering International (AACEI). Class 5 estimates are done where the requirements are not all specified or well understood. As such, some companies and organizations have elected to determine that due to the inherent inaccuracies, such estimates cannot be classified in a conventional and systemic manner.” Accuracy ranges for Class 5 estimates are 20% to 50% on the low side, and 30% to 100% on the high side.

**Consequently, a very high risk multiplier was applied to the 2008 analysis because the requirements for a biometric exit and the effort it would take to build an effective system were not defined or well understood at the time. We understand a lot more today and what once would have been a custom development (as estimated) can now predominately be performed by lower cost commercially available off-the-shelf (COTS) biometric solutions.**

Since 2008, US VISIT has matured and is better understood by the industry; interoperability between airline systems and DHS and CBP systems are better defined; and the biometrics industry has developed commercially available off the shelf tools and software which largely take the place of custom development which was estimated in the 2008 study. Consequently, our lower estimates are based on a more thorough understanding of the likely requirements surrounding a biometric exit strategy in the U.S. and is based on readily available commercial biometric technology.

There are many other factors associated with the 2008 study that are worthy of update that would also reduce the risk and associated costs.

In addition, there are other considerations to point out, pending the identification of the specific implementation objectives or requirements:

- The biometric cost component of the exit system is likely to be small relative to other costs like on-going staffing. Our industry makes many components as commercial-off-the-shelf (COTS), and prices have declined markedly over the last five years, while features and variety of offerings have increased.
- Under any operational concept, biometrics are the low cost solution because the US-Visit biometric infrastructure is already in place. The exit system is essentially adding input devices into the existing system for symmetrical operation (biometrics-in, biometrics-out). This is not the case for the proposed enhanced biographic system with secret personal questions. Not only is such a system less secure and subject to spoofing, but there is no infrastructure in place, nor are there any published estimates on the cost of such a system.
- There is a cost trade-off, depending on the operational concept, between increased staffing with low-cost mobile exit verification devices, vs. lower staffing with higher-priced fixed and automated electronic exit gates, called “e-Gates” or “ABC gates” (Automated Border Control gates).
- Depending on the airport gate structure for international operations, adding US-VISIT Exit infrastructure may actually lessen the load on airline personnel, if automated boarding pass processing is part of the function in an e-Gate implementation.
- There are different business models the industry can offer to help facilitate the establishment of an Exit capability. There is the obvious traditional technique of initial capital outlay with annual maintenance contracts. Increasingly, however, options are being offered for level service agreements, wherein the initial capital costs are amortized over a period, and a periodic service fee is charged to cover provision and maintenance of the equipment. Think of this as “US-VISIT Exit as-a-Service.”

### Reader costs

In determining the cost of readers necessary to fulfill a robust biometric exit requirement, we believe that the results of the 2008 US-VISIT “Air/Sea Biometric Exit Project Regulatory Impact Analysis” are useful as a starting point, if updated with the latest data from our industry. That analysis provided costs for 1,010 gates at the 73 airports and seven sea gates where CBP currently has personnel. It also assumed a total of 1,342 devices to cover multiple readers where throughput needs extra support due to high volume or potential reader malfunction. Of course we know that a likely implementation in 2015 would have different requirements and assumptions, and certainly very different component costs.

The reader costs provided below include software (but not system design and operations and maintenance). Each of the readers, at a minimum, would need to be configured to swipe two fingers and also be equipped with an MRZ (Machine Readable Zone) reader to scan travel documents (e.g. passports and boarding passes). We start with the simplest technology first (albeit requiring more attendant labor), and end with the most automated technology last (requiring the least attendant labor).

**FOR ORDER OF MAGNITUDE COMPARISONS ONLY**, we are showing the math for the total of 1,342 referenced in the 2008 study:

1. Portable fingerprint readers, with passport readers, on a cart that can be moved from lane to lane depending on which lane is assigned for foreign travelers and passenger throughput. Current costs range from \$3,000 to \$5,000. **One-time maximum cost (\$5,000/per reader x 1,342 readers) = \$6,710,000. Requires one attendant per reader during use.**
2. Hand held fingerprint readers, with passport readers, that can be used at lanes to facilitate passenger throughput. Current costs fall in the \$5,000 to \$7,000. **One-time maximum cost (\$7,000/per reader x 1,342 readers) = \$9,394,000. Requires one attendant per reader during use.**
3. Contactless fingerprint mobile readers (with passport readers) with costs in the range of \$8,000 to \$10,000. **One-time maximum cost (\$10,000/per reader x 1,342 readers) = \$13,420,000. Requires one attendant per reader during use.**
4. Automated e-Gates, to include passport readers and fingerprint readers. **Face and iris readers and boarding pass readers are options on some models. Prices range from \$50,000 per unit to \$150,000 per unit, depending on features and configuration ordered. One-time maximum cost (\$150,000/eGate x 1342 gates) = \$201,300,000. This option requires far less labor, since one attendant can monitor multiple e-Gates.**

Possible future options include face and iris biometrics, which DHS S&T, in cooperation with US-VISIT, has trialed for uses at border crossings. Prices for such features range from less than \$1500 per unit, up to about \$35,000 per unit for the most sophisticated stand-off iris readers. It should be noted that prices for iris readers are declining rapidly, particularly since the country of India has recently embraced iris as a primary biometric for their nationwide UIDAI Aadhaar identification project.

## Conclusion

Based on the successful and expanding use of biometric entry/exit systems worldwide and their acceptance by the public, along with the highly successful operation of US-VISIT biometric entry for more than a decade, which provides a solid infrastructure and foundation for a biometric

exit, the identification technology industry is confident that a biometric exit can be effectively implemented.

While properly subject to requirements definition and operational concept determination, we believe that cost effective biometric exit can be implemented now at U.S. international airports. Indications are that this could be done at a fraction of the dated DHS estimate. Designed and implemented properly, with good project management, such implementations not only support existing passenger throughput, but could actually enhance boarding operations of the airlines themselves, while minimizing impacts on Government personnel. We very much appreciate the opportunity to share this information with you, and look forward to working with you to implement this critical statutory mandate.