

Testimony before the
House Judiciary Committee

IMPLEMENTATION OF AN ENTRY-EXIT SYSTEM: Still Waiting After All These Years

Wednesday, November 13, 2013, 10 am

Janice Kephart

former Special Counsel, Senate Judiciary Committee (during
consideration of S. 744, *Border Security, Economic Opportunity, and
Immigration Modernization Act*)

former Counsel, National Commission on Terrorist Attacks Upon the
United States

Chairman Goodlatte, Ranking Member Conyers , as well as Border Security Subcommittee Chairman Gowdy and Ranking Member Lofgren, thank you for the opportunity to testify on the implementation of a biometric exit, a critical immigration, security and law enforcement issue that spans eight statutes and 17 years.

My name is Janice Kephart, and I approach the of border security and the entry/exit issue as a: former border counsel on the 9/11 Commission that proposed recommendation of a biometric entry/exit system; twice counsel to the Senate Judiciary Committee (in the late 1990s for the then Subcommittee on Technology, Terrorism and Government Information, and again during the 2013 consideration of immigration reform); as former National Security Director and now Fellow at the Center for Immigration Studies; as an specialist on identity and border security; and president of my own consulting firm, 9/11 Security Solutions LLC.

Summary

Tracking the arrival and departure of foreign visitors to the United States is an essential part of immigration control, with collateral effects on law enforcement and national security. The need for arrival controls is obvious, but recording departures is also important; without it, there is no way to know whether travelers have left when they were supposed to. Creating a feasible and cost-effective solution for foreign visitors has emerged as the linchpin in fully implementing the eight statutes first passed beginning 16 years ago.

It is also vital that such exit tracking employ biometric indicators — for instance, the travelers’ photos or fingerprints. Using only biographic information, such as names or passport numbers, provides no assurance that the person departing is the one whose original arrival was recorded. This testimony demonstrates that a biometric exit-tracking system for aliens departing by air or sea is feasible immediately at a reasonable cost, and a phased-in approach is available for land ports of entry. Due to the vast differences between air/sea and land ports of entry, they are treated as separate solutions.

It is a marked potential improvement that Customs and Border Protection is now responsible for implementation of a comprehensive biographic/biometric entry/exit solution. Their conclusion in the September 27, 2013 “Comprehensive Exit Plan” issued pursuant to the statutory requirements of the “2103 Department of Homeland Security Appropriations Act” is encouraging:

CBP is progressing on a fiscally conservative, thoughtful, and responsible path to deploy a comprehensive biographic and biometric entry/exit system.

CBP and DHS S&T continue to advance the research and development for potential biometric air exit program options and are identifying operational concepts that are

feasible in the current environment at U.S. airports and seaports. CBP and DHS S&T will begin testing concepts in early calendar year 2014, which will significantly inform future efforts.

Overall, DHS has significantly improved the existing entry/exit system throughout all operational environments and will further the biographic efforts while working toward a feasible biometric solution.

With DHS now actively working towards a solution that incorporates biometrics at air and sea ports, Congressional oversight and discussion is particularly welcome.

For brevity, a system that tracks the departure of foreign nationals will often be referred to simply as “exit”.

Implementing Biometric Exit at Air and Sea Ports of Entry

The first section of this testimony demonstrates that a biometric exit-tracking system for foreign nationals departing by air or sea is feasible immediately at a reasonable cost. This section is a reprint of my Center for Immigration Studies (CIS) report published in September 2013, ***“Biometric Exit Tracking: A feasible and cost-effective solution for foreign visitors traveling by air and sea”*** found [here](#), published in my current capacity as National Security Fellow at CIS.

Among the findings:

- The first-year implementation costs for all air and sea ports would range from \$400 million to \$600 million, even assuming significant cost overruns.
- This estimate is based on the current costs of existing devices and on the April 2008 [“Air/Sea Biometric Exit Project Regulatory Impact Analysis”](#).
- Implementation costs could be covered by a relatively small fee increase on foreign nationals arriving by air or sea and likely does not require an appropriation.
- Such a system could be implemented with minimal impact on the 40 million foreign visitors who travel by air.
- The Oct. 2009 Congressional report, [“US-VISIT Air Exit Pilots Evaluation Report”](#) that studied data from two airport biometric pilot programs concluded that “Overall, the Air Exit Pilots confirmed the ability to biometrically record the exit of aliens subject to US-VISIT departing the United States by air.” Today, technologies are faster, more diverse, and cost-effective.
- The Biometrics Institute (based in Australia), an international forum representing governments, suppliers and researchers in its published 2013 survey said that the number one most significant trend noted by its members for this year was Biometrics at the Border. In fact, 16 nations already have, or are in the process of implementing, biometric

processing of foreign air travelers including Ghana, while New Zealand has combined airline check-in and immigration control in its second generation system. The UAE has had no issues with its biometric border control at all land, air and sea ports since installation in 2004. Indonesia has implemented real time watchlist entry/exit biometric checks in six months at its largest airport that processes 10 million international passengers annually, just second in the U.S. to New York JFK's annual processing of 12 million. The list goes on.

- Congress has mandated the deployment of an exit-tracking system in eight separate statutes, starting in 1996. The three most recent laws require a biometric element. But the executive branch has so far refused to implement such a system.
- In contrast to the rejection of biometric exit-tracking at home, the same federal government is helping install biometric border systems abroad, in Nigeria and the Philippines.

Implementing Biometric Exit at Land Ports of Entry

The second section of this testimony describes biometric solutions at land ports of entry. The focus for implementation should be on 39 busiest land ports representing 95 percent of the total northern and southern border traffic. Tracking the departure of visitors by land is a very different challenge because of completely different conditions at land ports of entry versus air/sea ports of entry. To be clear, any movement on a biometric exit deployment on our northern border should be in counsel and cooperation with Canada, building on the good work in implementing a biographic entry/exit data exchange at northern land ports of entry, to the extent possible.

- A biometric exit-tracking system for foreign nationals departing by *pedestrians* at land ports of entry is likely feasible immediately at a reasonable cost, mimicking processing at air/sea ports of entry using interior locations at ports of entry.
- A biometric exit is feasible in the near future for *individuals and truckers already enrolled in trusted traveler programs* with little port infrastructure change and little cost. A straightforward solution duplicates the trusted traveler Radio Frequency Identification (RFID) technology used at entry lanes to exit lanes. No new IDs would require to be issued to these individuals.
- The backbone of the solution for *vehicular traffic* would be trusted traveler RFID technology that exists at entry replicated in exit lanes, "smart cards" that mimic the technologies, security and privacy features of trusted traveler documents. This type of solution was tested in 2005 by US-VISIT and the Smart Border Alliance, and determined to be feasible.
- The difference with a biometric exit solution and today's trusted traveler systems is that the verified departure data would be recorded and then relayed to Arrival/Departure and Advanced Passenger Information Systems.

- RFID and corresponding ID card technologies are proven, cost-effective and significantly better and relatively inexpensive.
- Using trusted traveler systems as a base model for biometric exit, the essential trade, facilitation and departure collection goals of border controls can be met, including incorporating the good work of DHS and Canada in their shared entry/exit information system and other cooperative border agreements that are maturing rapidly.
- For all foreign nationals seeking entry into the United States not currently enrolled in trusted traveler programs, the United States should strongly consider expanding the RFID / secure identity electronic framework into issuance of visas, border crossing cards, and other travel documents accepted to use for entry/exit across U.S. borders. According to the Smart Card Alliance, chips holding biometrics and RFID capable cost only a few dollars a piece.
- Cost for travel documents enhanced with biometrics and RFID capable could be folded into visa and other program fees.

Implementing Biometric Exit Air and Sea Ports

Developing and implementing a biometric exit capability to collect biometric data, such as fingerprints, which is required by federal law, has been a long-standing challenge for DHS. In May 2012, DHS internally reported recommendations to support the planning for a biometric exit capability at airports — DHS’s priority for biometric exit capabilities — that could also be implemented at seaports in the future. . . . DHS officials stated that the department’s goal is to develop information and report to Congress about the benefits and costs of biometric air exit options before the fiscal year 2016 budget cycle.

— “Overstay Enforcement: Additional Actions Needed to Assess DHS’s Data and Improve Planning for a Biometric Air Exit Program”, [GAO-13-683](#), July 30, 2013.

Introduction

This report attempts to show the way, for the first time, to a clear path toward a feasible, cost-effective biometric exit-tracking program at all air and sea ports of entry. The report concludes that a wide array of solutions are available immediately with a total first year implementation cost ranging from \$400 to \$600 million. This cost includes a 50 percent risk factor of \$125 million and is based on current industry device costs and a [2008 Department of Homeland Security \(DHS\) regulatory assessment of costs](#) associated with deploying biometric exit to all air and sea ports.

According to the U.S. Department of Commerce Office of Travel and Tourism Industries, approximately 40 million foreign visitors traveled by air to the United States in 2012, with overall travel and tourism to the United States up 7 percent. This level of traffic could be covered by an air and sea biometric exit system with minimal impact on individual travelers. In fact, small increases in visa waiver and visa application fees would cover costs without affecting

budget constraints. The more expensive options are unmanned solutions used around the world today, while the less expensive options can require higher ongoing labor costs. None require air carrier support or air/sea port infrastructure changes. All are proven technologies.

The results of a [2009 DHS evaluation report](#) that tested biometric exit solutions at two large U.S. international airports is further evidence that a biometric exit is feasible now. Moreover, at least 14 nations have or are deploying biometric border solutions at airports, and three nations have or are deploying biometric guest worker tracking programs. Some nations have had biometric solutions at all air, land, and sea ports for a decade, with superb results in data integrity and border control.

The key elements of a practical biometric exit program are reasonable, real cost estimates; tested and mission-capable technologies; and, in order to drive government accountability and long-term efficiencies in deployment, assurance that only immigration authorities will implement and collect the departing aliens' biometric information.

Biometric exit tracking is well established as a cornerstone of an efficient, enforceable immigration system. However, four main impediments to implementation remain in the United States. These are: (1) DHS's policy that the current biographic exit system, which relays departing flight manifest lists to immigration authorities, is sufficient for national security and law enforcement purposes; (2) unsubstantiated assumptions that costs would be exorbitantly high; (3) speculation that quick, accurate biometric processing of departing aliens is not feasible; and (4) refusal of the air carriers to abide by current law requiring air carrier collection of biometric exit data from departing aliens.

Eight statutes currently require an exit system. The three most recent statutory requirements all include a biometric element. However, despite a consistent reiteration of congressional intent to require a biometric exit program over the past decade and clear technological capability for deployment, the executive branch continues to refuse to implement such a system. This report seeks to dispel myths and put forth solutions on cost and feasibility, as well as to identify where legislative streamlining may be needed and assess the policy reasons for implementing biometric exit.

This report focuses on concurrent deployment of exit tracking for air and sea travelers. This is because carriers at seaports process departing foreign nationals in a similar manner to carriers at airports. The land solutions will be addressed in a separate report because of the different requirements for a different type of port of entry, one that must accommodate dense, incoming vehicular and pedestrian traffic, and outgoing traffic that currently undergoes little, if any, processing.

Biometrics in U.S. Border Management

Digital facial images and 10 fingerprints taken at air ports of entry and consular offices abroad of foreign nationals seeking admission into the United States are a cornerstone of U.S. border management. Biometrics also have become a foundation for intelligence and law enforcement

investigations within the United States. The biometric facial images and fingerprints taken at ports of entry are queried an average of 30,000 times every day by authorized federal, state, and local government users. The United States also shares some of this data with international partners such as Australia, Canada, New Zealand, and the United Kingdom to help apprehend international criminals and terrorists who have been caught trying to change their names and other biographic information in an attempt to find safe haven in the United States or one of these international partners.

According to DHS's US-VISIT (US Visitor and Immigrant Status Indicator Technology) [website](#), the purpose of taking biometric data at entry is to:

[A]ccurately identify people and determine whether they pose a risk to the United States. US-VISIT supplies the technology for collecting and storing biometric data, provides analysis of the data to decision makers, and ensures the integrity of the data. By using biometrics, US-VISIT is helping to prevent the use of fraudulent documents, protect visitors from identity theft, and stop thousands of criminals and immigration violators from entering the country.

US-VISIT was appropriated \$232 million and reorganized in the 2013 Homeland Security Appropriations Act. The office was divested of two difficult areas for which it had been responsible over the past decade that reflected more operational policy management than biometric development and integrity. These were (1) identifying visa overstays and determining visa overstay rates; and (2) the development and implementation of a biometric exit program.

U.S. Immigration and Customs Enforcement (ICE), which is responsible for enforcing immigration law against foreign nationals who overstay or violate the terms of their admission, is now responsible for identifying overstays and determining overstay rates. This workload would be minimal with a biometric exit, which would do much of the work for ICE and enable the agency to focus on enforcing the law rather than diverting hundreds of agents to this task as it does now.

The development of a biometric exit program is now squarely with Customs and Border Protection (CBP), which is already wholly responsible for biometric entry inspections. The only lost budget item in the 2013 DHS appropriations bill is US-VISIT losing its mission to support international partners in establishing their own US-VISIT-style programs, an understandable move at a time of tight budgets.

In the wake of 9/11, the purpose of US-VISIT was to eliminate passport and visa fraud by using biometrics to assure that those presenting travel documents at consular offices overseas during the visa application process, or those applying for admission at U.S. ports of entry, were who they claimed to be, a core recommendation in the 9/11 Commission report.

In 2013, appropriators in the House of Representatives gave US-VISIT a new name — it is now the Office of Biometric Identity Management (OBIM) — and rejected a budget request by the Obama administration to submerge US-VISIT in CBP. Essentially, House appropriators' refusal to accept the administration's budget request was an acknowledgment that US-VISIT had grown

well beyond its initial mandate, becoming a biometric program cornerstone serving immigration, law enforcement, and national security concerns equally.

The value of OBIM's biometric data will double when it acquires departure information from a CBP-implemented exit solution. Biometrically verified exit data will significantly augment OBIM's partners' ability to conduct investigations. This information can determine eligibility for an immigration benefit, for example. In other instances, biometric exit data can determine whether a foreign national deemed a threat is inside or outside the United States. This is not a hypothetical situation; whether a terrorist had departed was a key issue with two 9/11 hijackers two weeks before the attacks, where law enforcement gave up looking for watchlisted individuals on the incorrect assumption that they had already departed the United States.

More specifically, accurate and real-time exit data will support OBIM authorized law enforcement, immigration, and national security government clients as follows:

- [U.S. Customs and Border Protection](#) (CBP) uses OBIMOBIM's services at U.S. ports of entry to make sure the person seeking entry is the person to whom a visa was issued, to protect travelers against identity theft, to prevent fraudulent document use, and to ensure wanted criminals and terrorists are kept out.
- [U.S. Citizenship and Immigration Services](#) (USCIS) uses OBIM's services to establish and verify the identities of people applying for immigration benefits, including asylum or refugee status.
- The [U.S. Coast Guard](#) uses OBIM biometrics-based mobile services at sea by checking the biometrics of apprehended criminals and immigration violators on the spot, and using the data to prosecute illegal migrants and smugglers.
- The [Department of Defense](#) and the intelligence community use OBIM to compare latent fingerprints or other biometric information found during terror investigations to verify identities of known or suspected terrorists on watch lists.
- The [Department of Justice](#) and state and local law enforcement use OBIM's services to ensure that they have accurate immigration information about individuals they arrest; interoperability exists between OBIM's Automated Biometric Identification System (IDENT) and the FBI's Integrated Automated Fingerprint Identification System (IAFIS) fingerprint databases. OBIM's Biometric Support Center (BSC) helps many federal, state, and local agencies with their investigations by providing forensic biometric support 24/7. Some of these cases help solve crime and terror cases that may match records in state fingerprint database systems as well.
- The [Department of State](#) uses OBIM's services to establish and verify the identities of visa applicants at embassies and consulates around the world through its BioVisa program. Consular officers use this information in determining visa eligibility.

Statutory Authority

Various laws requiring exit control have sat on the books since 1996. In 2000, two separate laws were passed, one that established an exit system and one that tied it to the Visa Waiver Program. In 2001, the USA Patriot Act chimed in again, demanding exit. In 2002, the Border Security Enhancement law again required exit, and in 2004 the Intelligence Reform Act emanating from 9/11 Commission recommendations included a biometric exit. Beginning in 2004, and until 2007, pilot programs for exit were undertaken at the demand of Congress. The technology worked, but compliance rates were low since the kiosks were not clearly mandatory or placed in locations that required compliance.

In 2007, the 9/11 Commission Recommendations Act reiterated the need for exit and required exit apply to all foreign nationals entering under the Visa Waiver Program, adding in a biometric component and requiring the airlines to carry out the processing. In 2008, DHS put out a proposed rule-making for the [“Collection of Alien Biometric Data Upon Exit From the United States at Air and Sea Ports of Departure”](#), requiring the airlines to collect biometric data anywhere in the international departure process. The airlines refused. A viable exit system was far from implementation.

Today, there are three core statutes that provide the parameters of a biometric exit for air, sea, and land ports of entry. These are:

- The 2004 Intelligence Reform and Terrorism Prevention Act (8 USC § 1365b). This act streamlined the prior five statutory requirements for exit by defining a “biometric entry and exit data system” as the applicable sections of:
 1. The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (Public Law 104–208);
 2. The Immigration and Naturalization Service Data Management Improvement Act of 2000 (Public Law 106–205);
 3. The Visa Waiver Permanent Program Act (Public Law 106–396);
 4. The Enhanced Border Security and Visa Entry Reform Act of 2002 (Public Law 107–173) [8 U.S.C. 1701 et seq.]; and
 5. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Public Law 107-56).
- The 2007 9/11 Commission Implementation Act, Section 711, Section 217(i) of INA, of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), which places collection onus on air carriers.
- The March 2013 Department of Homeland Security Appropriations Act that requires Customs and Border Protection to implement a biometric exit program.

The 2004 Intelligence Reform and Terrorism Prevention Act. The [2004 law](#) begins as follows: “Consistent with the report of the National Commission on Terrorist Attacks upon the United States, Congress finds that completing a biometric entry and exit data system as expeditiously as possible is an essential investment in efforts to protect the United States by preventing the entry of terrorists.” The law requires full implementation of a biometric entry/exit system at all ports of entry by December 2004. More specifically, the 2004 law lists the “Entry-exit system goals” as follows:

The Department of Homeland Security shall operate the biometric entry and exit system so that it:

1. Serves as a vital counterterrorism tool;
2. Screens travelers efficiently and in a welcoming manner;
3. Provides inspectors and related personnel with adequate real-time information;
4. Ensures flexibility of training and security protocols to most effectively comply with security mandates;
5. Integrates relevant databases and plans for database modifications to address volume increase and database usage; and
6. Improves database search capacities by using language algorithms to detect alternate names.

All immigration component databases held by ICE, CBP, USCIS, the Department of Justice’s Executive Office of Immigration Review, and State’s Bureau of Consular Affairs were to be integrated with the biometric exit system. By December 2006, a fully interoperable electronic data system, as required by Section 202 of the Enhanced Border Security and Visa Entry Reform Act (8 U.S.C. 1722), was to provide standardized “current and immediate access to information in the databases of federal law enforcement agencies and the intelligence community that is relevant to determine — (A) whether to issue a visa; or (B) the admissibility or deportability of an alien.” Guidelines were also provided for assuring the security of the data, and enabling correction of erroneous data by the public.

Further seeking to implement core 9/11 Commission recommendations, the 2004 law required that entry/exit data be available electronically and used in determining immigration benefit application outcomes, including visas, work permits, immigration court cases and investigations, and creating a tracking system tied to the biometric identifier to assure accurate identification of applicants or those under investigation.

The 2007 Visa Waiver Program for Certain Visitors. [Section 217\(h\)](#) of Immigration and Nationality Act was amended in 2007 to require air carriers to “collect and electronically transmit” passenger “arrival and departure” data to “the automated entry and exit control system” developed by the federal government. Deployment of an exit system was also tied to further expansion of the Visa Waiver Program. The exit requirement was ignored, however, by

both the Bush and Obama administrations, which both actively expanded the Visa Waiver Program without a biometric exit program.

The 2013 Homeland Security Appropriations Act. For 10 years Congress has tried to force DHS to establish an exit program to no avail. US-VISIT was involved with the issue because of a statutory call for a biometric exit. Being the only true biometric and immigration program office in the federal government, US-VISIT was saddled with conducting exit pilots and rendering massive reports that the current administration has refused to make public. Meanwhile, CBP, which only in the past few months has been made responsible for full implementation of a biometric exit program, was included in pilots and contributed input, but never had final say, control, or accountability for getting the job done. In the [2013 Homeland Security Appropriations Act](#), the appropriators took the issue off the table and made clear that CBP is fully in control, and also accountable, for planning and deploying a biometric exit program.

The appropriators also finally streamlined the various legal requirements pertaining to exit and set forth a viable, practical, phased approach that was desperately needed. CBP now has clear marching orders: the agency must produce an enhanced biographic exit system first, and quickly, with a later phase-in of a biometric exit system. While it is unnecessary to continue with a biographic system considering the maturity of biometric border exit solutions currently available (see below), the good news is that the agency that is responsible for border inspections at entry, is now also the responsible agency for the border inspections at exit.

One more potential benefit of the new shift of overstay analysis to ICE and exit implementation to CBP: This change may cause the necessary friction to actually make exit happen. ICE relies on many forms of exit data now, but getting the same data in the same manner with the same standardized information consistently from CBP would make ICE overstay operations much more efficient. However, that will likely require either the Obama administration to develop and implement a biometric exit system, or significant congressional oversight that is satisfied only with results, not excuses for failing to implement a program first required 17 years ago. Below is the current budget allocation for OBIM from the 2013 Homeland Security Appropriations Act, which clarifies the new set of responsibilities for OBIM, CBP, and ICE relative to biometric exit program development (emphasis added):

OFFICE OF BIOMETRIC IDENTITY MANAGEMENT

A total of \$232,422,000 is provided for the “Office of Biometric Identity Management.” This level includes: \$40,546,000 for Salaries and Expenses (S&E); \$15,980,000 for Systems Engineering; \$155,840,000 for Operations and Maintenance (O&M), to include \$65,500,000 for IDENT; and \$20,056,000 for Identity Management and Screening Services. ... The bill provides \$19,917,000 to ICE in order to fully fund overstay analysis previously performed by US-VISIT, to include the Data Integrity Group. The bill also provides \$12,284,000 to CBP related to entry-exit policy and operations.

Implications of a Biometric Exit on National Security and Overstays

As mentioned in the introduction, 40 million foreign nationals visit the United States by air annually. This number represents nationals from visa waiver countries where the United States does not require a visa for tourism or business travel lasting 90 days or less from the [current list](#) of 37 qualified countries. The 40 million also includes anyone from a Visa Waiver country that is applying outside of tourism or short-term business, as well as any country that is not in the Visa Waiver Program.

National Security. Little has changed on progress to implement an exit program since the 9/11 Commission made this finding of fact in its [9/11 and Terrorist Travel](#) monograph: “On August 23, 2001, the CIA provided biographical identification information about two of the hijackers to border and law enforcement authorities. The CIA and FBI considered the case important, but there was no way of knowing whether either hijacker was still in the country, because a border exit system Congress authorized in 1996 was never implemented.”

Not having an exit system in place led the 9/11 Commissioners to conclude in 2011 that our border system must include data about who is leaving and when, with the following recommendation: “The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system. As important as it is to know when foreign nationals arrive, it is also important to know when they leave. Full deployment of the biometric exit . . . should be a high priority. Such a capability would have assisted law enforcement and intelligence officials in August and September 2001 in conducting a search for two of the 9/11 hijackers that were in the United States on expired visas.” (See [“Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations”](#)).

Our more recent experience with terrorist threats and attempts reiterates the commissioners’ point. In the wake of the Christmas Bomb Plot and the near-getaway by would-be Times Square bomber Faisal Shahzad (who had already boarded a flight to leave the United States when he was arrested), we are once again reminded that a biometric exit system is needed to prevent a terrorist from “fooling” the system and getting away.

Overstay Enforcement Efforts and the Visa Waiver Program. Biometric exit is a key component to assuring the integrity of the Visa Waiver Program, by assuring that overstay rates are accurate and readily available to determine either a nation’s qualifications to be accepted into the program or its continued participation in it. The fact that DHS officials told the GAO during its investigation for the May 2013 report [“Immigration Enforcement: Preliminary Observations on DHS’s Overstay Enforcement Efforts”](#) that there remains no confidence in the current biographic data system, is strong evidence that a biometric system is needed to support the Visa Waiver Program.

More specifically, the inadequacies of visa overstay analysis today make clear that biographic data alone are inadequate in assuring the identity of foreign nationals coming and going through the immigration system. According to the May 2013 GAO report referenced above, there are currently more than one million “unmatched arrival records” in the DHS’s Arrival and Departure Information System (ADIS), or potential cases where immigrants may or may not have remained in the country with expired visas, and cannot be identified.

Foreign air travelers benefit from accurate data regarding their arrivals and departures because it minimizes errors that may affect future travel. The relationship between overstay data and the need for a biometric air exit was further emphasized in the July 2013 GAO report “[Overstay Enforcement: Additional Actions Needed to Assess DHS’s Data and Improve Planning for a Biometric Air Exit Program](#)”, which notes the following:

In 2011, DHS reviewed this backlog of 1.6 million records, closed about 863,000 records, and removed them from the backlog. As new unmatched arrival records have accrued, DHS has continued to review all of these new records for national security and public safety concerns. As of June 2013, DHS’s unmatched arrival records totaled more than one million. ...

Federal law requires DHS to report overstay estimates, but DHS or its predecessor has not regularly done so since 1994. In April 2011, GAO reported that DHS officials said that they have not reported overstay rates because DHS has not had sufficient confidence in the quality of its overstay data. In February 2013, the Secretary of Homeland Security testified that DHS plans to report overstay rates by December 2013. However, DHS has not assessed or documented improvements in the reliability of data used to develop overstay estimates, in accordance with federal internal control standards. Without such a documented assessment to ensure the reliability of these data, decision makers would not have the information needed to use these data for policy-making purposes.

Terrorist overstays are also a significant issue, which, under the current system, can be tracked down only through difficult, tedious, and time-consuming investigations. Recent terrorist overstays include Hosan Smadi, a Jordanian national who plotted to blow up a Dallas skyscraper in 2009, and Amine El Khalifi, a Moroccan whose visa expired in 1999, who was arrested in an attempt to bomb the U.S. Capitol in 2012.

Assuring Identity. These one million “unmatched” records would likely not exist, or be substantially reduced, with biometrics. Biometrics enable identity to be verified instantly and eliminate the risk of missing a threat due to the misspelling of a name or other biographic errors. Instead, biometrics allow instant, real-time assurance that people are who they say they are. Biometrics also prevent identity theft, preventing the swipe of lost or stolen passports from being used to manipulate the system as to who has actually left the country.

Instant, verified overstay data would give CBP and the State Department better information to determine who gets to visit the United States again, and ICE better information about who returned or illegally overstayed. Exit data would also support all current customers of OBIM biometric data, and may even give Joint Terrorism Task Forces the ability to curtail terrorist absconders who slip out of the United States unnoticed based on verified watchlist hits — akin to the attempted escape by the Times Square bomber, who was boarded and on the jetway when apprehended, having bypassed a biographic-only exit system and TSA security.

U.S. Supports Biometric Border Programs Abroad. Although the federal government currently does not have a biometric exit program, the United States is actively supporting biometric border programs in both Nigeria and the Philippines. In April 2013, a U.S. delegation

arrived in Nigeria to discuss [installation of a biometric system](#) through its Ministry of the Interior to help secure its borders, with the overall goal of stemming the tide of rising insurgency and helping to stabilize the Nigerian regime. According to Dwight Brown, the U.S. delegation program manager, “You can change your name, you can get a new passport, but you can’t change your fingerprints and this system checks the fingerprint of every traveler that comes through it. . . . Our system is powered by biometrics and fingerprints, the most powerful identification technology available today.” The Nigerian newspaper report noted that “The technologies will be provided by the USA while the Nigeria Immigration Service personnel will be trained to man them.”

In April 2013, the United States [donated two fingerprint scanners](#) to the Philippines Bureau of Immigration at the Ninoy Aquino International Airport to take fingerprints of all arrested aliens and build a photo and fingerprint biometric database of illegal aliens and foreign fugitives wanted by immigration intelligence personnel. A Filipino immigration official commented that “This will prevent these blacklisted aliens from re-entering the country even if they assume a different name, use a different passport, or disguise their physical appearance.” The country’s Immigration Commissioner thanked the U.S. government for its support in upgrading its facilities and enhancing the Filipino authority’s ability to enforce immigration laws.

Biographic Only vs. Biometric Plus Biographic

There continues to be a debate over whether a “biographic-only” approach to exit is sufficient. But that is essentially the system currently in place, whereby advance passenger data and name records of foreign nationals who have checked in for departure are logged into the immigration arrival-departure database. As discussed, a biographic-only system has numerous problems, including the inability to confirm identity. The only way to confirm identity is through biometric means such as facial recognition software, iris scans, and fingerprints. This section explores the policy and practical reasons as to why, in each instance, a biometric solution is the only one that provides the benefits for government, the traveler, the airport, and the airline (or, in the case of the sea ports, the sea carrier).

The Problem with Names. A serious issue that remains unsolved more than a decade after 9/11 is misspelled or inaccurately recorded names. The 19 hijackers collectively had over 300 spellings of their names. Recently it was discovered that Boston Marathon bomber Tamerlan Tsarnaev’s name was misspelled on a manifest list of a flight to Russia, meaning that the FBI did not have the benefit of an important lead in investigating his terrorist ties. Problems with the biographic-only approach continue despite software to help correct misspelled names. Simply requiring a “next generation” version of such software will not solve the problem; merely enhancing software that picks up name anomalies can never be sufficient because thousands of varieties of uncommon names from all over the world are spelled differently in English or even purposefully misspelled. Nor does such software pick up complete biographic identity changes, a much more nefarious problem that biometrics solves in seconds.

Identity verification produces actionable information. When an individual purchases a plane or boat cruise ticket, the federal government (indeed, most all governments) require advance passenger identity information, including Passenger Name Records (PNR) taken by airlines.

This information is then turned over to government authorities for risk assessments. Upon arrival at the airport for departure, the identity associated with the passenger must be verified. The seconds it takes to process a biometric solution is essential to assuring that the name matches the individual, eliminating nearly all varieties of fraud.

Without biometrics, either no vetting occurs or it is simply a name-based vetting, which is both inaccurate and unable to be fully verified. The result is inordinately long — sometimes hours — queues for a slow, manual, and inaccurate process carried out by overworked border agents.

However, automated, unmanned departure zones that scan biographic passport data and capture biometrics provide biometric identity verification within seconds by matching it against the biometric information obtained at entry, which in the United States is a digital photo and 10 fingerprints. Departure requires only verification against one of these biometrics. Using fingerprints as a base for a U.S. system, for example, would require verification of only two prints, a much quicker and easier solution than already exists at air ports at entry.

Using the same device — a set of monitored kiosks, unmanned gates, or handheld devices — passport data would be scanned concurrently with whatever biometric was captured. This data can be matched against the advanced passenger information and PNR data, and identity and biometrics can be vetted against existing law enforcement, intelligence, and watchlist information.

This does not mean that “hits” will result in a denial of departure or secondary inspection. In fact, that is not the point of an exit program. Instead, an exit program’s primary purpose is to record a confirmed departure that enables better decision-making by immigration, law enforcement, and intelligence authorities after the fact. But that does not mean real-time departure data could not be acted upon, which may be essential during an active criminal or intelligence investigation where the foreign national sought represents a significant flight risk.

Focus on High-Risk Passengers with Better Information. The current TSA document check neither confirms identity nor authenticity of a passport (or any other travel document presented). An option could be to place a biometric solution at the front of the TSA checkpoint, replacing the current check by a TSA agent with a mandatory biometric-biographic identity check and departure record that would enable security personnel to focus on high-risk passengers and enable the majority of low-risk passengers to go through a more streamlined security process, improving throughput rates. At the same time, high-risk passengers can be given informed additional security checks that aid aviation safety and immigration departure information integrity. The result would be a better-informed and more secure aviation environment while fulfilling a federal mandate of a biometric exit system.

In 2008, US-VISIT conducted an in-depth “[Air/Sea Biometric Exit Project Regulatory Impact Analysis](#)”. In comparing a biographic-only exit to a biometric exit, the assessment concluded that biometric was a far better choice for the following reasons:

- **Overstays.** The ability to determine overstays with the current biographic-only air exit is difficult and “the likelihood is high that not all overstays are identified.”

- **Failure to confirm identity.** “Reliance on biographic data, such as matching the name provided by the traveler to stored names, is fraught with risk.”
- **Incomplete immigration records.** “Without accurate and immediate recording of an in-scope traveler’s exit, the traveler’s entry-exit record is not complete. A risk exists that the traveler will be admitted into the United States without sufficient understanding of his or her entry-exit history.”
- **Ability to expedite entry.** “When the entry-exit, identity, or watch list information on a traveler is not current or accurate, or if the CBP officer does not trust the data, the CBP officer may request the traveler be sent for secondary inspection more often than would otherwise be the case. This delays the entrance of the specific traveler and potentially the admission of other travelers.”
- **Effects admission/participation of Visa Waiver Program countries.** “The database of entry-exit records of in-scope travelers risks being incomplete. Thus, calculation of exit compliance is not accurate.”
- **Supports resource allocation decisions for law enforcement officers.** “Confidence in the entry-exit record of the in-scope traveler would be increased if the collection of exit data and recording of exit data were automated, and the identity of the in-scope traveler could be assured.”

Solution

A biometric air/sea exit solution is available right now, as it was in 2009. It requires no infrastructure changes to airports, and can be deployed immediately. Neither TSA nor airlines need be directly involved; CBP should be fully responsible for implementation, management, and processing, as required under the 2013 Homeland Security Appropriations Act. Today, unmanned options that require only monitoring and customer support are available. The system would inform immigration law enforcement on overstays and reduce enforcement costs, and inform intelligence and law enforcement officials of terrorist and criminal departures.

The air/sea exit solution is based on biometric and airline industry queries, an extensive review of both the June 2009 US- VISIT Air Biometric Evaluation and the 2008 regulatory cost analysis by US-VISIT, and a review of both mature and newly implemented biometric border-control solutions deployed internationally.

Note that CBP, responsible for border protection and inspection within DHS, has conducted multi-modal biometric air entry processing since 2007 (based on a photo and 10 fingerprints). The current entry processing had significant infrastructure, interview, and biometric requirements that were successfully implemented — all of which are not required for an air/sea exit deployment. Solutions are mobile, manned or unmanned, and employ proven technologies that can facilitate processing of large volumes of foreign nationals without any significant

impediments to travel. In short, deploying a biometric exit solution is much easier to put in place than the biometric entry solution installed in 2005.

Key Elements of a Successful Deployment

Review of All Relevant Materials. Recent industry letters to Congress — listed as appendices at the end of this report — provide information specifically on cost and feasibility. The first is a detailed letter and separate memo from leading biometric provider, Safran MorphoTrak, formerly Sagem Morpho, which services the Automated Fingerprint Identification Systems (AFIS) in 28 states and 30 counties as well as immigration biometric entry/exit systems internationally. The second is a detailed letter from the International Biometrics & Identification Association relating current costs for full deployment of an air/sea biometric exit, and a “myths vs. facts” sheet. The last section of this report summarizes international deployments of biometric border solutions.

Applicability Only to Foreign Nationals. Departure requirements would not apply to U.S. citizens, but rather only to foreign nationals, including (1) foreign visitors seeking visas at consular offices overseas; (2) legal immigrants seeking immigration benefits in the United States; and (3) any foreign nationals granted temporary legal status, including those enrolled in any amnesty program.

Use of Proven Technologies. Air and sea infrastructures should integrate proven passport capture and biometric technology currently used in international immigration settings, by OBIM, and by U.S. law enforcement. Numerous vendors offer off-the-shelf mobile, kiosk, and e-gate fingerprint, facial recognition, and even iris and retina scan technologies. Fingerprint scanners, for example, are available as both contact and contactless and would be rather easily incorporated into OBIM’s existing fingerprint system management. Some operate as quickly as two seconds. The goal is to minimize cost, maximize speed, and assure the integrity of the departure data while protecting the data’s privacy and security.

“Exit” Data Captured. The system would link the reading of the passport and fingerprint data captured at the port of entry in real time to the existing Arrival and Departure Information System, the same system used now to record biometric entries and receive electronic manifest departure data.

Mobile Infrastructure and Technologies. Air and sea ports should be given a menu of options listing a handful of approved technologies that will most efficiently ensure an exit protocol that achieves immigration control without exorbitant costs or flow-through issues. Kiosks, e-gate zones, and handheld devices are all potential options, depending on the different needs of various jetway configurations. Such options exist currently at air, sea, and land ports around the world today.

International Air Travel Statistics. [According to the Department of Commerce](#), the fee revenue should continue to rise if air exit is deployed within the next two to four years. The April 2013 press release reads “U.S. Commerce Secretary John Bryson today announced that the United States can expect 4-5 percent average annual growth in tourism over the next five years, and that 65.4 million foreign travelers are projected to visit the United States in 2012 alone. The

Spring 2012 Travel and Tourism Forecast, released semi-annually by the U.S. Commerce Department's International Trade Administration (ITA), predicts continued strong growth through 2016 following two consecutive visitor volume records set in 2010 and 2011."

The 65 million foreign visitors include all entries by air, and sea, as well as those land entries that are recorded (many are not, since passport inspection of vehicle passengers is visual, unless there is a secondary inspection referral). Statistics on foreign air travelers are provided by the Commerce Department's Office of Travel and Tourism Industries in "[International Visitation to the United States: A Statistical Summary of U.S. Visitation \(2012\)](#)". The report's statistics show that all air visitors — most of whom are now required to pay security application or visa application fees — totaled 39.6 million. The breakdown is as follows: Air visitors from Canada increased 3 percent from 2011 to 2012, with 7,695,000 visitors in 2012; air visitors from Mexico increased 9 percent from 2011 to 2012, with 2,117,951 visitors; and all other nations combined increased 7 percent from 2011 to 2012, with 29,761,038 total overseas visitors.

To clarify further that most of the increase in the entry of foreign nationals will likely be by air, this same report summarized the countries of origin where tourism is currently increasing the most: "Top inbound countries with the largest increases in visits in 2012 were: the People's Republic of China (excluding Hong Kong) (+35 percent), Colombia (+21 percent), Venezuela (+20 percent), Argentina (+20 percent) and Brazil (+19 percent). All five countries set new records for visits to the United States." Near all entries from these countries are by air.

Funding. A \$10 increase in the current \$14 Electronic System for Travel Authorization (ESTA) fee for a newly created Bio-metric Exit Trust Fund, for a total fee of \$24, could be implemented to cover costs. ESTA is a tax paid by Visa Waiver applicants for pre-admission screening when they make travel plans to the United States. Current law requires that only \$4 of the fee be used by CBP to support the ESTA program, while \$10 is used by "Brand USA" to promote tourism to the United States. Another \$10 for a biometric exit — the same amount already provided to promote tourism — should not be too much to ask to help enforce the nation's immigration laws and implement a recommendation of the 9/11 Commission to ensure our security.

In addition, a \$10 increase in visa application fees for those foreign nationals not eligible for Visa Waiver status would cover the remaining costs. Applicants in many visa categories spend well over \$100 already. Another \$10 is a modest addition considering all the other costs of travel and immigration.

Based on the current level of foreign air arrivals, without even taking into account the projected increases in foreign tourism, these fee increases could raise \$400 million in the first year alone, more than enough to deploy an air/sea exit solution in a quick, phased approach over two years, and without incurring debt.

Any funds left over could be used to maintain and improve exit, implement full interoperability of immigration databases with other immigration components, and to enforce immigration law against visa overstays.

Feasibility

This section covers the feasibility, cost, and background issues for immediate, full implementation of a biometric air/sea exit program. In 2009, congressional appropriators required two airport biometric pilot programs before appropriating further monies for exit. One pilot tested handheld biometric-biographic devices at TSA checkpoints at Atlanta’s Hartsfield-Jackson International Airport, the other required CBP to screen departures with mobile laptops configured for a biometric-biographic exit on the jetway at Detroit Metropolitan Airport. Both worked well. Airlines refused to participate in the pilot programs, reiterating the argument that exit, like entry, is primarily a government function.

The study’s conclusion was: “Overall, the Air Exit Pilots confirmed the ability to biometrically record the exit of aliens subject to US-VISIT departing the United States by air.”

In the one month of processing between June and July 2009 — heavy international travel times — the study found that “The Customs and Border Protection pilot at the jetway in Detroit processed 9,448 aliens and identified 44 watch list hits and 60 suspected overstays. The TSA pilot processed 20,296 aliens subject to US-VISIT and identified 131 watch list hits and 90 overstays”, for an aggregate of “hits” of 1.10 percent for the CBP pilot and 1.09 percent of the TSA pilot.

The study also found that line lengths at the TSA checkpoint did not increase, and CBP officers on the jetway had little to no impact on departure times. The biometric exit solutions caused no costs or delays in travel queues that increased flight delays or resulted in missed flights. In addition, 99.99 percent of those identified to participate in the study, did participate — only one person in 30,000 refused. The study further found that DHS databases were able to maintain the quality and matching requirements using the fingerprints collected, assuring that people were who they said they were, and their exit data correlated to their identity.

This pilot program verified that a successful biometric exit can be as minimal as providing a fingerprint match and passport “swipe” to assure identity of a travel document holder who has departed. Exit deployment is thus significantly less complicated than the biometric entry system in place today that takes a digital photo and 10 fingerprints of each of the annual 170 million foreign visitors. Since the 2009 pilots, technology has significantly improved, cost has declined, and options — including unmanned but mandatory multi-modal (more than one biometric) biometric-biographic solutions — are in operation around the world.

Technology Today Is Better, Faster

Biometric technology is significantly improved over the 2009 US-VISIT findings:

- Processing is significantly faster, requiring less than two seconds for fingerprint capture in some cases and many complete biographic-biometric options operating in less than 20 seconds for full processing. In contrast, biographic entry operates at about a minute per traveler, and even in 2009 full processing was expected to take 66 seconds per passenger.

- Many solutions are multi-modal, allowing a simultaneous read of the digital photo stored in an e-passport matched against a real time facial image taken during departure, alongside a fingerprint scan that conducts a match against arrival fingerprint records, and the input of biographic passport data. Some systems also upload watchlists and cull in real time, for security purposes.
- Mobile units designed for flexibility and efficiency, enable throughput to be maximized based on the volume of passengers and assuring that no infrastructure changes are required. These mobile units can come in a variety of formats, including handheld devices, see-through lightweight “e-gates”, and mobile kiosks.
- Most systems are unmanned, enabling self-checkout, fast throughput, the highest levels of security, passenger convenience, and high efficiency for border personnel.
- Systems are fully encrypted to protect privacy and data integrity.

Eliminating Air Carriers from Processing

The 2007 Visa Waiver Act places collection of biometrics squarely on air carriers. To date, the air carriers have successfully blocked implementation of any exit program that places the onus of collection on the carriers, citing hidden costs, slowing of throughput, and passenger dissatisfaction. From an oversight perspective, the chief concern of Congress should be to eliminate air carrier concern by simply voiding the current mandate that the air carriers collect biometric data of departing aliens. Not one country in the world currently requires air carriers to collect this data, and for good reason: air carriers should not be in the business of administering immigration inspection, which is a government function.

Moreover, if CBP already conducts thorough biometric inspections at entry, that same entity should be ultimately responsible for implementing, managing, and processing “inspections” at exit. As enforcement action will not take place at exit except in exigent circumstances, few personnel will be required. In exceptional cases, such as a terror investigation, the FBI would likely be the arresting authority, not CBP. All in all, there is no reason to involve air carriers in processing or enforcement due to information arising from data acquired during departure.

Deployment to All Air Exits

While about 40 percent of international travel is concentrated in the United States’ top 30 international airports, the remaining 40 international and other airports slowly accrue the remainder of international air travel. Thus, any solution must incorporate these smaller volume airports. The easiest way to do so would be to minimize manpower and airport outlay by simply enabling smaller airports to install mandatory kiosks or e-gates as a subset of the security processes already in place, taking the place of the current TSA “document check”. At larger air and sea ports, where CBP already has manpower deployed for biometric entry, minimal manpower would be necessary to ensure compliance and customer support.

Table 1. International Passenger Throughput at U.S. Airports

Int'l. Vol. Rank	Total Vol. Rank	City, State	Airport	International Passengers (2012)	Percent of Total	Cumulative Percent
1	6	New York, N.Y.	John F. Kennedy	12,362,982	7.228	12.674
2	12	Miami, Fla.	Miami	9,314,482	5.446	17.534
3	3	Los Angeles, Calif.	Los Angeles	8,312,655	4.860	20.795
4	14	Newark, N.J.	Newark Liberty	5,577,111	3.261	23.75
5	2	Chicago, Ill.	O'Hare	5,055,210	2.955	26.542
6	1	Atlanta, Ga.	Hartsfield-Jackson	4,775,512	2.792	29.205
7	7	San Francisco, Calif.	San Francisco	4,554,495	2.663	31.679
8	11	Houston, Texas	George Bush Int.	4,231,034	2.474	33.56
9	23	Washington, DC	Washington Dulles	3,216,822	1.881	35.252
10	4	Dallas/Ft. Worth, Texas	Dallas/Ft. Worth	2,893,161	1.692	35%
Top 10				60,293,464		
11	27	Honolulu, Hawaii	Honolulu	2,175,234	1.271	36.523
12	19	Boston, Mass.	Logan	2,017,761	1.179	37.702
13	18	Philadelphia, Pa.	Philadelphia	1,857,908	1.086	38.788
14	13	Orlando, Fla.	Orlando	1,819,449	1.064	39.852
15	21	Ft. Lauderdale, Fla.	Ft. Lauderdale-Hollywood	1,681,772	0.983	40.835
16	17	Detroit, Mich.	Detroit Metropolitan	1,567,832	0.917	41.752
17	15	Seattle, Wa.	Seattle-Tacoma	1,546,825	0.904	42.656
18	8	Charlotte, N.C.	Charlotte Douglas	1,449,033	0.847	43.503
19	9	Las Vegas, Nev.	McCarran	1,392,926	0.814	44.317
20	10	Phoenix, Ariz.	Sky Harbor	1,097,825	0.642	44.959
Top 20				76,900,029		45%
21	16	Minneapolis, Minn.	Minneapolis/St. Paul	1,081,820	0.632	45.591
22	5	Denver, Colo.	Denver	869,908	0.509	46.1
23	20	New York, N.Y.	LaGuardia	728,847	0.426	46.526
24	22	Baltimore, Md.	BWI Thurgood Marshall	272,250	0.159	46.685
25	28	San Diego, Calif.	San Diego	264,694	0.155	46.84
26	31	Portland, Ore.	Portland	239,359	0.14	46.98
27	29	Tampa, Fla.	Tampa	217,092	0.127	47.107
28	43	San Antonio, Texas	San Antonio	209,343	0.122	47.229
29	25	Washington, DC	Ronald Reagan	190,208	0.111	47.34
30	26	Chicago, Ill.	Midway	188,144	0.11	47.45
Top 30				81,161,694		47%
31	24	Salt Lake City, Utah	Salt Lake City	182,281	0.107	47.557
32	40	Santa Ana, Calif.	John Wayne	122,906	0.072	47.629
33	30	Cleveland, Ohio	Cleveland Hopkins	99,280	0.058	47.687
34	38	Raleigh-Durham, N.C.	Raleigh-Durham	94,539	0.055	47.742
35	42	San Jose, Calif.	Norman Y. Mineta	83,955	0.049	47.791
36	34	Oakland, Calif.	Oakland	68,405	0.04	47.831
37	45	Pittsburgh, Pa.	Pittsburgh	60,089	0.035	47.866
38	46	Milwaukee, Wisc.	General Mitchell	47,037	0.028	47.894
39	39	Sacramento, Calif.	Sacramento	44,546	0.026	47.92
40	32	St. Louis, Mo.	Lambert	27,629	0.016	47.936
Top 40				81,992,361		48%
Total Int.				171,039,012		

This table was derived from Bureau of Transportation statistics of international passenger flow determined by querying the departure information by searching each of the "all major airports" and then querying all other international airports to determine a ranking in terms of 2012 international passengers departure throughput [here](#). The total international passenger throughput for all airports is found at the same link, by clicking "all" in the airport search engine in the top right search. The ranking for airports and initial determination as to the largest airports, was taken from the 2012 North American (ACI-NA) top 50 airports spreadsheet found on the Council for International Airports' [website](#). The percentages were determined based on this information.

[Footnote reprinted to include links]:

This table was derived from Bureau of Transportation statistics of international passenger flow determined by querying the departure information by searching each of the “all major airports” and then querying all other international airports to determine a ranking in terms of 2012 international passengers departure throughput [here](#). The total international passenger throughput for all airports is found at the same link, by clicking “all” in the airport search engine in the top right search. The ranking for airports and initial determination as to the largest airports, was taken from the 2012 North American (ACI-NA) top 50 airports spreadsheet found on the Council for International Airports’ [website](#). The percentages were determined based on this information.

CBP should be encouraged to engage airports to choose the most cost-effective solutions for their infrastructure and passenger throughput needs. Flexibility in solutions would allow airports with CBP to choose from an approved menu of solutions depending on airport infrastructure design and the large differences in throughput that would best fit the needs of particular departure jetways. The same would be the case for seaports.

According to Department of Transportation statistics on international air travel at 150 U.S. airports that provide international service, over 171 million passengers departed from the United States on international flights in 2012. In 2012, the top 10 airports represented about 35 percent of international departures, while the top 20 only increased the throughput by another 10 percent, at 45 percent of that travel. The top 30 airports represented 47.5 percent of that travel. The top 40 airports represented only 48 percent of that travel, a significant drop in volume. The remaining middle- and smaller-sized international airports only have a few thousand international departures annually. All totaled, 110 of the 150 airports together amount to 52 percent of the international departure traffic, with each producing less than a 1/2 of 1 percent of all traffic.

For example, John F. Kennedy Airport in New York receives almost 12.4 million international passengers annually. In contrast to JFK, Minneapolis, ranked 20th, at 1,081,000 international departures, produced just 10,000 in volume to JFK’s December 2012 throughput of 1,071,000. Miami, ranked second, produces significantly less volume than JFK at just over 9.3 million. Washington, D.C.’s Dulles Airport ranks 9th, at just under 3.2 million. The top 30th airport, Washington D.C. Ronald Reagan Airport ranks at 190,000 per year. New Orleans (not in Table 1) ranks at 50, with only about 22,000.

Cost

Industry Costs. The International Biometrics & Identification Association (IBIA) calculated its cost range based on the same 2008 DHS cost study used in the cost chart in this report, concluding costs of approximately \$9 million for handheld fingerprint/passport readers (requiring an immigration inspector to man each device) to \$200 million for biometric and boarding pass/passport reader e-Gates (requiring only one immigration inspector to man many devices at one time). These cost estimates were obtained by Sen. Jeff Sessions (R-Ala.) from industry representatives during consideration and markup of immigration reform legislation. The goal was to answer cost and feasibility questions regarding implementation of a biometric exit. The information attached to this report from Morphotrak and the IBIA are reproduced here with

the senator's express permission. Morphotrak's cost estimates for the top international airports representing 40 percent of the international traffic is \$90 to \$150 million for hardware and software depending on the solution chosen, including customization.

Added Values that Reduce Costs in Other Government Functions. The 2008 "Air/Sea Biometric Exit Project Regulatory Impact Analysis" noted the following improvements over a biographic exit system provided by an air/sea biometric exit system that provided added value and reduction in overall costs to the immigration system and national security:

- "Improved detection of aliens overstaying visas" (300 ICE agents do overstay analysis today).
- "Cost avoidance resulting from improved Immigration and Customs Enforcement (ICE) efficiency attempting apprehension of overstays" (in 2007, costs for removal per visa violator was \$18,375 per individual).
- "Improved efficiency of processing Exit/Entry data".
- "Improved national security environment".

Manpower and Other Costs. Manpower costs for CBP to assure and support processing would vary depending on choice of biometric solution; some mobile solutions require only monitoring and support, thus significantly reducing CBP manpower costs. The more popular international choice, e-gates, require little or no manpower. Handheld devices, in contrast, require a reader per inspector.

Total First Year Deployment Cost. Aggregating the 2008 US-VISIT impact analysis data and industry data, the greatest total cost for first year technology implementation would be approximately \$400-600 million, depending on collection units chosen. The more expensive units do not require an attendant per reader, but a single monitoring attendant who can supervise a number of mobile kiosks at once.

- The 2008 US-VISIT analysis assumes that the solution would be deployed to 73 international airports and 33 seaports, for a total of 11,990 individual devices (9,248 at airports and 2,742 at seaports). This may be significantly higher than actually necessary considering today's new e-gates and kiosk technology. Thus, the 2008 numbers here are likely significantly higher than actual cost for deployment.
- The 2008 analysis also calculated costs based on a 66.6 second processing time per alien. This number today would likely be less than 20 seconds per alien.

Table 2. Costs for Full Deployment to 73 International Airports and 33 International Seaports

Description	Cost	2008 US-VISIT Regulatory Impact Analysis for Biometric Air/Sea Deployment- Table Reference
Program Management	\$59,830,000	A-7 (15 percent of total program cost, as remainder resides with provider)
Independent Verification and Validation	\$1,990,000	A-8 (1% of total program cost)
Site Surveys for Air and Sea Ports	\$5,054,000	A-9
IDENT (Fingerprint) Upgrades (Storage and Match)	\$12,458,000	A-10
CBP Development Costs	\$3,473,000	A-11
Arrival Departure Information System Upgrades	\$2,447,000	A-12
Application Development	\$126,958,000	A-13
Software Testing	\$18,054,000	A-17
Software Deployment	\$12,164,000	A-19
Develop and Test Hardware	\$2,896,000	A-24
Data Communication Circuits	\$225,000	A-25
Network Connectivity Costs	\$9,220,000	A-26
Travel Delays	0	2009 US-VISIT Air Pilot Exit Evaluation Report found no travel delays in two different air biometric exit environments
Risk Factor	127,385,000	Assumes a 50 percent risk factor on unanticipated development/deployment costs
Training of CBP and Government Partners Using Exit Solution	\$2,139,000	A-35
Outreach	\$10,000,000	A-36 (5 percent of total program cost less program management, devices and training costs)
Subtotal	\$394,293,000	
Total range for collection device for fingerprint and passport Morphotrak/IBIA	\$9,394,000 to \$201,300,000	Lowest handheld reader costs and highest e-gate costs (as per International Biometric & Identity Association)
Total	\$403,687,000 to \$595,593,000	

- The 2008 analysis determined that about 52 million aliens would exit each year through air and sea ports, which is significantly more than entering today.
- This chart does not include airport infrastructure change costs, as these are not necessary with mobile solutions.

- Personnel costs are not included, as current solutions require only monitoring for multiple machines, not an attendant per device; the 2008 assessment included over 5,000 attendants required for all air and sea ports assuming an attendant per device for 18 hours a day, seven days a week at airports, and six hours a day, four days a week at seaports at about \$60,000 per officer or about \$300 million annually. In addition, costs were based on average salaries for air carrier personnel, not CBP. Thus, it was impossible to transfer or use personnel costs from the 2008 assessment. However, assuming three agents for every four gates at \$50,000/year/agent, that cost would be about \$39 million annually. The ongoing personnel cost as determined by CBP is easily covered by relatively small ESTA and visa fee increases as discussed above.
- Technology costs for air carrier collection of data, and transfer of that data between air carriers to the government, is not relevant as it was in 2008.
- Time per foreign national enrollment in exit average about one minute or more in 2008; that time is now reduced to anywhere between two seconds and twenty seconds per foreign national, also reducing both technology and labor costs.
- The 2008 analysis calculated the devices at \$7,700 apiece for a total of \$35.5 million in cost. The price of the devices discussed in this report vary, depending on the solution provided.
- Morphotrak costs were recalculated for full deployment, using the DHS numbers in the 2008 assessment of 106 combined airports and seaports. This report assumes that CBP would require the same deployment to the same listing of airports.
- High-end collection devices require only supervision of multiple devices at once, not collection and personnel per reader.
- Costs not included from the 2008 assessment are either no longer relevant without air/sea carrier involvement nor infrastructure changes needed, or would be covered by the provider.

Biometric Systems Worldwide

The United States has failed to create the efficiencies and effectiveness that the rest of the world is realizing in biometric entry/exit systems. In fact, The Biometrics Institute (based in Australia), an international forum representing governments, suppliers and researchers in its published 2013 survey said that the number one most significant trend noted by its members for this year was Biometrics at the Border. The solutions vary from fingerprint and facial recognition devices to iris scan technologies; from manned to unmanned stations; from land to air to sea programs; from guestworker to entry/exit solutions. Biometrics is considered the foundation for optimization of passenger processing, and thus integral to the future trend in airline and immigration processing where the mission is to increase self-service, drive efficiencies, reduce queues, and simplify processing for passengers.

For example, Saudi Arabia has been using iris recognition technology since 2002 to manage the huge influx of visitors during the Hajj, using the system to both enhance security and prevent visa overstays. One vendor already has 30 government clients for its automatic facial recognition border solutions throughout the world. Another vendor verified in a 2010 DHS National Institute of Standards and Technology report that it has excellent facial recognition software for border control environments, which is now being installed throughout the European Union. Some places, like Amsterdam, are already on their second-generation deployment of biometric border controls.

Biometric border systems are not necessarily concentrated in developed countries; less-developed countries are deploying, or have already deployed, biometric systems to control their borders. Some are doing so with help from the U.S. government. Others are doing so with next-generation technologies. Some international airlines are testing biometrics to replace paper tickets and multiple presentations of travel documents prior to boarding. In the United States, Chicago O'Hare International Airport recently began automating some of its immigration controls for arrivals. The most advanced systems, such as New Zealand's second-generation deployment, are integrating airline check-in and boarding with immigration entry/exit. This section summarizes many of those advances.

International Airport Entry/Exit Systems

Biometric entry and exit immigration systems are deployed worldwide to enhance security, customer experience, and facilitation. Some countries, such as New Zealand, are deploying second-generation systems that incorporate passenger check-in and ticketing. Facial recognition, iris, and fingerprint technologies all provide amplified benefits and relatively negligible differences in speed and accuracy from each other; all are markedly better than any "enhanced biographic" system. Many of these systems are unmanned, and while immigration or customs officials are on site to conduct inspections as necessary, their deployment is efficient, allowing the technology to conduct exit data recording and identity verification, while facilitating processing of all others.

Abu Dhabi. Abu Dhabi was one of the first countries to deploy a biometric border entry/exit system. Its primary purpose was to make sure that those "expelled" from the country did not change their name, obtain a new passport, and return with a new identity that a biographic system could not discern. From a 2004 article:

Over a distributed network involving all 17 air, land, and sea ports into the Emirates, the iris patterns of all arriving passengers are compared in real-time exhaustively against an enrolled central database. According to the Ministry of Interior, which controls the database, so far not a single false match has been made, despite some 2.7 billion iris cross-comparisons being done every day.

On a typical day, more than 6,500 passengers enter the UAE via seven international airports, three land ports, and seven sea ports. By looking at an iris camera for a second or two while passing through immigration control, each passenger's iris patterns are encoded mathematically and the resulting IrisCodes sent over a distributed

communications network to a central database controlled by the General Directorate of Abu Dhabi Police. There they are compared exhaustively against an enrolled database of 420,000 IrisCodes of persons who were expelled from the UAE for various violations, many of whom make repeated efforts to re-enter the UAE with new identities using forged travel documents. Thus the current daily number of iris cross-comparisons performed under the UAE expellee tracking and border-crossing control system is about 2.7 billion. It is the first system of its kind in the world, with more than 2.1 million arriving passengers already checked in this way. The time required for each passenger to be compared against the full database of registered IrisCodes is less than one second.

So far more than 9,500 persons have been caught by this system travelling with forged identities. According to Lt. Col. Ahmad Naser Al-Raisi, Director of the Information Technology Department at the General Directorate of Abu Dhabi Police, “We found the system to be very effective and extremely fast. Its speed, accuracy, and ease-of-use enabled us to deploy the project without difficulties.”

Australia. U.S. Global Entry members can now use a new biometric gate system, based on a combined protocol between U.S. and Australian Customs and Border Protection using facial recognition technology. These e-gates are similar to the ones deployed in New Zealand (see description below). U.S. Global Entry is a CBP “trusted traveler” program that allows expedited clearance for pre-approved, low-risk travelers upon arrival in the United States who, instead of standing in line for inspection by a border agent, can enter the United States by using automated kiosks located at select airports. Rigorous background checks are required for participation. Upon arrival, Global Entry participants scan their machine-readable passport or U.S. permanent resident card at the kiosk, place their fingertips on the scanner for fingerprint verification, and make a customs declaration. The kiosk issues the traveler a transaction receipt and directs the traveler to baggage claim and the exit.

Bulgaria. Bulgaria’s Sofia Airport has installed automated border clearance using both e-passports and facial recognition technologies that process passengers in 7-10 seconds. The new gates are available for European and Swiss travelers over 18 years of age. Border inspection desks still exist for those who do not qualify for the expedited processing.

Canada. The Canada Customs and Revenue Agency began using iris recognition technology for frequent travelers at Toronto and Vancouver International Airports in 2003. The Expedited Passenger Processing System uses iris recognition technology to conduct matching on those pre-registered with the system, which includes both Americans and Canadians registered in the trusted traveler NEXUS program. Today iris recognition technology is used to verify visitors through NEXUS at eight major Canadian international airports in addition to Vancouver, at Calgary, Edmonton, Winnipeg, Toronto, Ottawa, Montreal and Halifax.

Czech Republic. The Czech Border Police’s installation of an entry/exit e-gate system at Prague’s Vaclav Havel Airport won the Czech Republic’s “IT Project of the Year” in 2012. The Czech Minister for the Interior said this about the system: “The EasyGo project is a practical example of how biometric IDs can be used. The highly developed solution offers a self-service for crossing the border with a high level of security and saves the passengers time.” The

software solution combines individual biometric components such as passport readers or cameras with background systems. According to the vendor, crossings are completed in an average speed of 18 seconds per person. The system has already had over 130,000 passengers from European Union countries use the system.

Ireland. The Irish Naturalisation and Immigration Service and Dublin Airport Authority implemented an automated facial recognition border control gate pilot at Dublin Airport beginning in May 2013, verifying that the passport holder is the same individual seeking to enter Ireland and is authorized to do so. The system operates in about 7.5 seconds and the pilot is processing about 1,000 passengers per day. Authorities are already noting that staff workload is reduced, document fraud is better prevented, and border control waiting times are reduced. If verification fails, the passenger is led directly to the manual passport control without blocking the passenger flow. A spokesman for the vendor said, “There needs to be more convergence, too — the sharing of information between airports, airlines and authorities. Using biometrics for identification could lead to more secure, more comfortable and faster processes.”

Alan Shatter, Minister for Justice, Equality and Defense, commented: “Border control arrangements at Dublin Airport are currently undergoing major change. Immigration control processes are being reviewed and leading-edge border technology such as automated gates is being tested. Many major European airports are adopting a similar trend towards the deployment of automated gates for immigration control functions to enhance passengers’ experience on arrival at airports while also strengthening border security.”

European Union. European Union member states began implementation of recommendations to move to self-service border control using automated border control gates that incorporate facial recognition, and optionally fingerprint verification, run against e-passport data for verifying the passport belongs to the passenger. The EU recognizes that unmanned gates that only require manual intervention by an immigration officer in rare cases when a match is unsuccessful reduce immigration personnel requirements and wait times, increase airline activity, and produce more revenue at the airport. The particular face recognition algorithm used by the EU is listed as one of the best by the National Institute of Standards and Technology (NIST), in testing commissioned by DHS.

Ghana. With the help of the World Bank, Ghana Immigration Services (GIS) is implementing an electronic visa and border management electronic entry/exit gate solution that will enable intelligence and law enforcement information sharing in real time. Ghana has become increasingly concerned with its cross-border traffic, and will now be able to supervise and manage an automated passport inspection while recording border crossings using entry and exit data recorded into the system. All ports of entry will be automated, including Accra’s Kotoka International Airport. In addition, Ghana is deploying a biometric visa processing system.

France. Paris’s major international airport, Charles de Gaulle, now has 33 fingerprint automated border gates since deployment after a successful 2009 pilot. These gates have processed more than one million individuals departing France since their installation. The French claim that e-gates are a win-win, with passengers spending more time shopping in duty-free areas and shorter lines. The e-gates assure that only one person is in the gate, detect abandoned luggage, and then

verify the passenger's identity. In 2012, French citizens holding biometric passports could also use the gates.

The success of the program has resulted in the first deployment to a regional airport, the [Marseille Provence airport](#). "We will now be targeting deployment of our systems in other international airports throughout France," explained Jean-Paul Jainsky, Morpho Chairman & CEO. "With a very low rejection rate — less than 3 percent — and proven technology, biometric gates are an iron-clad investment. In the future, other biometrics such as face or iris registration, might be added to the PARAFE system, it should make life easier for the millions of travelers using European airports."

[Indonesia](#). A biometric border solution installed at nine airports and one seaport in Indonesia in October 2011 can match and manage up to 20 million unique biometric identities. The first installation was completed in six months in one of Indonesia's largest airports that handles 10 million international passengers a year. The system provides real-time matching against a biometric watch-list. The technology is multi-modal, "capturing face and fingerprint data of arriving travelers and manages it in a person-centric database of identities. Duplicate identities are consolidated into a single person record allowing people who are claiming multiple identities to be easily tracked. This data is used by all departments to prevent identity fraud, including controlling the issue of stay permits, and managing primary line operations and illegal migrant activity."

[Latvia](#). Self-boarding gates at Riga International Airport allow passengers to use a combination of iris, fingerprint, and facial recognition biometric technologies to validate identity and process information. The gates can process both a printed boarding pass as well as a digital boarding pass displayed on a smartphone. "This project enabled us to provide a better service to those visiting us and at the same time improve the overall airport operational efficiency and passenger flow. In the first day of operation the self-boarding gates served more than 1,000 passengers and the objective is for this number to continue to rise," according to Raimonds Arajs, Riga Airport's IT Director.

[The Netherlands](#). The first deployment of a biometric border entry system was in October 2001 when an iris recognition system was installed at Amsterdam's Schiphol Airport. The system expedites the way for travelers from 18 European countries into the Netherlands, including frequent travelers in a two-phase process. Enrolled travelers pay \$89 annually for the service, which allows them to bypass long immigration lines. Similar to U.S. land border trusted traveler programs, passengers undergo a background check and a passport review. Users also undergo an iris scan. The template is encrypted and embedded on a smart card. This phase takes about 15 minutes but once the passenger has the smart card, it can be used for each entry through Schiphol airport. Once the individual has the smart card, instead of standing in line, the smart card is scanned at the immigration checkpoint, identifying and verifying the registered traveler. Each time the smart card is scanned, it is compared with a real-time scan of the iris. This process typically takes about 10 to 15 seconds.

In 2006, the system was [upgraded](#) for a quicker process for both arrivals and departures with improved security, deploying automated border control e-gates that use facial recognition

technology to verify identity against the digital photo embedded in the e-passports. As of January 2013, one million travelers have used these automated border control e-gates at Schiphol. There are a total of 36 units at the airport, located in the Departure 3, Arrival 3 and transit areas between Schengen and non- Schengen.

New Zealand. The New Zealand Customs Service has rolled out a next generation of SmartGates at its largest airport, Auckland International, an upgrade to their SmartGate system implemented in 2009. As of July 2013, six million passengers have used the current system, and more than 70 percent of those eligible to use the system do so. Customs officials state the technology is so precise that it allows them to focus on high-risk travelers while everyone else has an improved experience.

The latest version of the SmartGate creates a one-step concept for both boarding and security. The passport is scanned at the gate, eliminating the need for the kiosk and ticket. SmartGate Plus is a Morpho Australasia product that uses “face-on- the-fly” technology. A three-dimensional facial image of a user’s face is taken as the individual approaches the gate and then compares it to the image stored in a presented e-passport. The individual barely has to slow down while the technology uses a 3D facial recognition for matching. The new system will be available for passengers over 16 years old carrying a New Zealand, Australian, U.S., or UK e-passport.

Saudi Arabia. At the King Abdul Aziz Airport in Jeddah, Saudi Arabia, iris recognition tracks and identifies the entry and exit of visitors on pilgrimage for the Hajj season of worship. The process includes a random check at passport control, database enrollment, and subsequent identification on departure. The systems ensure that visitors do not overstay their visas and also identify potential security threats.

Taiwan. In 2008, Taiwan set up a three-in-one fingerprint, face, and retina biometric system for Taiwanese nationals at major airports in 2008 at a cost of \$1.2 million. The Taiwanese Ministry of the Interior is currently extending biometric immigration capture to both “unregistered” Taiwanese and foreign nationals at a cost of \$6 million. This system will use a dual facial recognition and fingerprint technology captures. The purpose is to assure that departures have occurred and verify identity.

In comparing the new biometric system to a “photo tool,” the Taiwanese Minister Chia-chi said: “Plastic surgery can change the way a person looks, but it cannot change biological features such as the distance between two pupils,” Chia-chi said. “If the system fails to identify the person by comparing facial features, we would then check their fingerprints.”

To date, more than 9,400 foreign nationals living in Taiwan registered for the new automated system. As of May 27, 40,459 entries and exits had been made through the e-gate system by foreign residents in Taiwan. Altogether, over 5.08 million entries and exists by both Taiwanese and foreign nationals have been recorded through the e-gates since the system was launched in 2011.

United Kingdom. The United Kingdom’s Border Agency is requiring Manchester Airport to capture facial images of all departing passengers upon both entry into the departure terminal,

and again upon leaving the terminal, to assure that identity and immigration data is accurate and verified prior to boarding. Anyone refusing compliance is denied boarding.

Biometric Guest Worker Systems

[Australia](#). Frustrated by illegal workers, overstays, visa fraud, and a \$4 billion annual cost of identity fraud, Australia's immigration, law enforcement, and intelligence services now have access to digital fingerprints and photos from driver's licenses, nightclubs, and passports. In addition, facial recognition and fingerprint software is required to verify worker eligibility. "According to the report in [AustraliaForum.com](#), employers convicted of employing illegal workers face fines up to \$13,200 and two years' imprisonment while companies face fines of up to \$66,000 per illegal worker."

[India](#). India is testing securing its maritime borders with biometric smart cards. BiometricUpdate.com notes that, "Set to start in September 2013, 800 local fishermen will initially be included in the test and an estimated 300,000 more would be covered. Reported in *The Hindu*, the government plans to use card readers at "harbour and authorized fish landing centres for authorities to verify the identities of fishermen, in an attempt to [prevent] terrorists from entering mainland India."

[Singapore](#). Iris recognition is used to admit workers who travel into Singapore from Malaysia each day by motorcycle. The workers' irises are scanned by a camera installed in kiosks in designated lanes, instead of their having to present their paperwork to an official. About 50,000 workers cross the border each day.

Airline Boarding Systems

U.S. airlines have long fought current statutory requirements that require air carriers, not immigration authorities, to support departure processing of foreign nationals. Their arguments included that immigration is a government, not a commercial function; slows facilitation; decreases customer experience; and creates associated costs. All of these arguments are valid. However, assuming the inevitability of an exit system, the airlines have also supported a biographic departure system over a biometric solution for the same reasons of perceived slower processing and decreased customer satisfaction. International competitors of U.S. air carriers are proving the falsehood of these perceptions.

Instead, cutting-edge international air carriers are taking lessons learned from biometric border management and beginning to apply them to passenger check-in and boarding. These carriers recognize that enhancing security while decreasing hassle for travelers in a more seamless airport environment creates a safer and less stressful experience for everyone. Travel and tourism need not be pitted against security. Instead, biometric solutions pave the way for better business models for government, airports, and commercial airlines when identities are quickly verified, airlines require less or no paper tickets, and airports have the opportunity for increased commerce from the time saved with biometric border and check-in solutions.

Referred to as "SmartGates", "e-gates", or "self-boarding", airlines in conjunction with international airports are beginning to test biometric boarding for the similar reasons as

immigration authorities, to gain efficiency, facilitation, and heightened security simultaneously. International airlines and airports now see biometrics as the wave of the future, speeding up processing, reducing paper, and assuring identity. Heathrow Airport is the first to use these gates for airline processing.

United Kingdom. South African Airways is working in conjunction with London's Heathrow Airport in a "self-boarding" program that requires airline staff to only check a passenger's identity once during the departure process. Using self-boarding gates, passengers pass through an automatic electronic barrier that takes an infrared scan of their face. This information is checked against the biometric data that was taken at the check-in stage. If the data matches, the barrier opens and the passengers can pass through and board their flights. A Heathrow press release notes the following:

The technology means that a passenger's identity needs to be checked by airline staff only once in the whole departure process, reducing the time it takes for passengers to get to their seats ready for take off. It also allows airline staff to spend more time with those passengers who require greater assistance. The personal data is stored securely and will be destroyed at the end of the trial.

Heathrow's Terminal One director, Ian Hanson, said this: "We are working in partnership with our airlines to trial this technology which should help make our passengers' journeys smoother and simpler. Since its introduction we have had positive feedback from both airlines and passengers." These gates are produced by the same company that built the Schiphol Airport e-gates that have processed over a million passengers.

Automated Customs Entry for U.S. Citizens at Chicago's O'Hare Airport

In May 2013, Chicago O'Hare became the first U.S. airport to implement a customs declaration kiosk that allows U.S. citizens to fill out a digital customs declaration, doing away with the paper cards provided on airlines prior to arrival. The 32 kiosks were provided by the Vancouver Airport Authority, which had recently undergone a successful trial of the kiosk technology, and installed on July 1, 2013. The touch-screen kiosks ask passengers a series of questions, then produce a paper receipt. The receipt is then presented to CBP personnel upon leaving baggage claim along with the current procedure of showing passport and boarding pass. The kiosks are free and require no prior registration. The automated procedure is designed to speed up departure from arrival zones.

According to Chicago Mayor Rahm Emanuel, "This technology will help expedite customs processing for passengers arriving to O'Hare, further strengthening Chicago as a global destination. Being the first airport in the U.S. to implement these advances demonstrates how serious we are about making Chicago the first, best and most welcoming city in the country."

While not a biometric solution and significantly less technologically advanced than other nations' biometric SmartGate and kiosk solutions, the endorsement and implementation of automated immigration procedures at an American airport by a major political figure is a significant step in the right direction, and bodes well for the nonpartisan nature of an automated, biometric exit solution.

BIOMETRIC INDUSTRY LETTERS



919 18TH STREET, NW, SUITE 901, WASHINGTON, DC 20006 USA

TEL 202.587.4855 FAX 202.587.4888 * WWW.IBIA.ORG

June 5, 2013

Re: US- VISIT Biometric Exit

Dear Senators:

The Honorable Jeff Sessions

326 Russell Senate Office Building Washington, DC 20510

The Honorable John Cornyn 517

Hart Senate Office Building Washington, DC 20510

The Honorable Dianne Feinstein 331

Hart Senate Office Building Washington, DC 20510

The Honorable Orrin G. Hatch

104 Hart Senate Office Building Washington, DC 20510

The Honorable Mike Lee

316 Hart Senate Office Building Washington, DC 20510

The Honorable Marco Rubio

284 Russell Senate Office Building Washington, DC 20510

On behalf of the members of the International Biometrics & Identification Association, comprised of the leading global providers of identification, we would like to thank each of you for your commitment and interest in fulfilling the mandate in both federal and regulatory law for implementing a biometric exit control system for foreign nationals. We appreciated your joint leadership and public commentary during the Senate Judiciary Committee markup of S. 744, “Border Security, Economic Opportunity, and Immigration Modernization Act.”

As S.744 heads to the Senate floor for consideration, we are sending this letter to provide you with the specific information you requested on the feasibility of implementing a biometric exit as well as the cost of implementing the mandatory program.

In summary, the 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:

- 1 This is not an untried program. Such systems are commonplace around the world.
- 2 US- VISIT has been highly successful, providing a strong foundation for a biometric exit.
- 3 Biometric exit leverages the biometric enrollment at US- VISIT entry.
- 4 Biometric exit will be simpler and more efficient than other suggested solutions and will
- 5 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 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. Figure 1 shows an example of an automated e- Gate installation, such as might be used at the entrance to an international terminal (after the security checkpoint) or to 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. **(This estimate is for 73 airports and seven seaports and not the 10 airports in the Senate bill.)** 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 significantly overstated.

Most significantly, the 2008 study designated their 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 at all 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 biometric exit and the effort it would take to build an effective system were not 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 estimate is based on a more thorough understanding of the likely requirements surrounding a biometric exit strategy in the U.S. and is based readily available commercial biometric technology.

There are many other factors associated with the 2008 that are worthy of update that would 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.

- 1 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).
- 2 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. 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. We understand that not imposing additional work on airline personnel is a key issue for that industry’s acceptance of an Exit function.
- 3 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.
- 4 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.”

5 Reader costs

- 6 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.
- 7 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
2. 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.**
3. 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.**
4. 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) = \$13,420,00. Requires one attendant per reader during use.**
5. 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 US- VISIT Biometric Exit Page 8 of 8

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 resolve this critical statutory mandate.

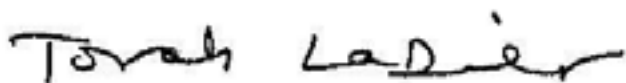
We hope this information is useful and would be pleased to review this with you and any questions and requests for further information.

We greatly appreciate the opportunity to provide this data to you and look forward to working with you to implement this important national security program.

Sincerely,

Tovah LaDier

IBIA Managing Director





113 South Columbus Street, Suite 400 Alexandria, VA 22314

Tel: (703) 797-2600

Fax: (703) 706-9549

June 5, 2013

The Honorable Jeff Sessions

326 Russell Senate Office Building Washington, D.C. 20510

The Honorable Dianne Feinstein 331 Hart Senate Office Building Washington, D.C. 20510

The Honorable John Cornyn 517 Hart Senate Office Building Washington, DC 20510

The Honorable Mike Lee

316 Hart Senate Office Building Washington, DC 20510

Re: Biometric Air Exit Solution

Dear Senators Sessions, Feinstein, Cornyn, and Lee:

On behalf of MorphoTrak, I want to thank you for your leadership and public support for biometrics in an immigration setting. Biometrics is and always will be the best means to assure identity. Right now, we are able to deploy an effective and viable biometric air exit system using proven technologies without inconveniencing foreign nationals departing on international flights. We appreciate the opportunity to provide this information as requested.

Who is MorphoTrak

MorphoTrak is a world leader in multi-biometric technologies and an acknowledged expert in identification systems. Our solutions meet a wide range of security needs for people, companies

and governments worldwide. We are a U.S. company with about 500 employees dedicated to biometric product innovation, project implementation, and customer support.

Our headquarters are in Alexandria, VA, with large facilities in Anaheim, CA and Federal Way, WA.

MorphoTrak provides the FBI with fingerprint matching solutions including those used in the new Next Generation Identification (NGI) System. MorphoTrak has also deployed and currently supports Automated Fingerprint Identification System (AFIS) solutions for law enforcement in 28 states and over 30 cities and counties, including the New York (City) Police Department, New York State, Florida Department of Law Enforcement, Harris County and the City of El Paso Texas, Arizona Department of Public Safety, Orange County California Sheriff's Department, Colorado Bureau of Investigation, Missouri State Highway Patrol, New Jersey State Police, North Carolina State Bureau of Investigation, South Carolina Law Enforcement Division, State of Wisconsin Department of Justice, and a large array of interoperable AFIS systems across the U.S. National Capital Region and surrounding jurisdictions.

Biometrics Used for Immigration

Biometrics serve as the basis for OBIM (formerly known as US-VISIT), which today is used to take a digital photo and 10 fingerprints for all foreign nationals that enter at US ports of entry. There are currently over 150 million visitors in OBIM that are queried an average of 30,000 times a day by the Department of Homeland Security, Department of Defense and state, local and federal law enforcement and intelligence agencies to verify identities and identify potential criminals and terrorists.

The results of the "2009 US-VISIT Air Exit Pilots Evaluation Report" that Senator Sessions made public during the Senate Judiciary Committee markup of S. 744, "Border Security, Economic Opportunity, and Immigration Modernization Act", clarify that an air biometric exit mandate could have been fulfilled in 2009 without operational or compliance issues that plagued the earlier January 2004 to May 2007 pilot. Biometrics can provide the level of security needed to have a cost-effective and comprehensive system for both entry and exit.

Feasibility of Implementing Biometric Air Exit

MorphoTrak is part of a global corporation which deployed large-scale biometric intake and matching systems for immigration purposes including Automated Border Control Solutions (ABCS) installed recently in 9 countries at 20 international airports. These systems include the Australia and New Zealand SmartGates, the French Parafe, UK IRIS, and UAE Abu Dhabi systems processing in excess of 700,000 passengers per month. MorphoTrak is currently the only biometric provider capable of fielding a contactless fingerprint capture technology (also known as "finger-on-the-fly") ideally suited for high-throughput immigration and border control applications.



WHAT: The purpose of utilizing biometrics as the foundation of a comprehensive exit program is to accurately match non-U.S. citizen departure data with previously collected arrival information. The exit solution requires the collection of a biometric (i.e. fingerprints), along with biographic data, from foreign nationals in order to enable biometric matching and identity verification at departure gates and/or TSA security checkpoints.

HOW: Non-U.S. citizen visitors with an international destination are directed to areas near the departure gate or at the TSA checkpoint for biometric information collection. Using a mobile or portable (cart-based) collection device (such as finger-on-the-fly), the officers collect one or more fingerprints electronically. The fingerprints can be matched locally on the collection device or remotely. A biometric match returns the associated biographic information that is then compared with the biographic data in the Machine Readable Zone (MRZ) of a passport, such as name, country, passport number and date of birth. In the attached estimates, we assume 23 airports for our calculations which comprise 40% of the international travel from the U.S.

PRIVACY: All data remains encrypted during the entire transmission process. High level security protocols and procedures are used to protect all devices and data used by CBP, TSA or other officials.

SmartGate Sydney, Australia Facial Recognition Border Control

MorphoTrak suggests the use of contactless, “on-the-fly” biometric capture that enables agents to be reassigned to tasks that require manual intervention. The contactless fingerprint technology does not require a passenger to stop walking to place their hands on a device or be touched by an agent. This maximizes passenger processing, eliminates hygiene concerns and can alleviate cultural or religious objections.



MorphoTrak's Finger-On-The-Fly

By using contactless fingerprint and/or advanced biometric handheld technologies, the exit process can be expedited, resulting in less than 2 seconds for fingerprint capture for each passenger. All of these technologies are available today.

MorphoTrak has included an attachment identifying costs for multiple options to enable a biometric exit system. These estimates include options for (1) mobile devices, (2) biometric kiosks with contactless fingerprint capture, (3) exception handling, (4) 1:1 and 1:few biometric searching for those foreign nationals who do not have biometric passports, (5) mirror copy of the US VISIT (OBIM) database, and (6) migration of the US VISIT databases.

MorphoTrak believes that the biometric portion of an exit program could fall within the range of \$90,000,000 to \$150,000,000 using a combination of the options mentioned above.

MorphoTrak greatly appreciates your support and would be pleased to provide any additional information you require.



Sincerely, Clark Nelson



Senior Vice President MorphoTrak, Inc.

CORPORATE HEADQUARTERS

113 South Columbus Street, Suite 400 Alexandria, VA 22314

Implementing Biometric Exit at Land Borders

The feasibility and cost of a biometric land port of entry exit solution depends on the type of departure, existing infrastructure capabilities, and ability of the biometric exit to fulfill statutory mandates that enhance the integrity of our border system while continuing to support trade and tourism. Despite the challenges, a biometric exit is feasible in a phased-in approach. Biometric exit controls for foreign national pedestrians and trusted travelers could be implemented relatively quickly, while non-trusted traveler vehicular traffic would take longer.

An obscure 2005 joint US-VISIT and Smart Border Alliance study of land exit using RFID-embedded secure credentials proved that even at that time, an ID could be read at 50 mph under good circumstances. Eight years later the technology is better and more accurate. The concept is similar to EZ-PASS in place on highways and the trusted traveler systems today that operate today at the 39 busiest land ports that represent 95 percent of total northern and southern border traffic. It is these ports that should be prioritized for biometric exit deployment.

To be clear, any movement on a biometric exit deployment on our northern border should be in counsel and cooperation with Canada, building on the good work in implementing a biographic entry/exit data exchange at northern land ports of entry, to the extent possible.

Key elements for a successful land biometric exit implementation include:

- **Use of proven technologies for quick, well-executed deployment.** Incorporating proven technology, including useful elements of five different trusted traveler programs, for a quicker, well-executed and trusted deployment.
- **Applicability.** Departure requirements would not apply to U.S. citizens. The departure requirement would apply to all foreign nationals, including (1) foreign visitors seeking visas at consular offices overseas; (2) legal immigrants but for those exempted by law; (3) any foreign nationals granted temporary legal status, including those enrolled in any amnesty program.
- **Secure Credentialing.** For those visiting and departing by air or sea, the secure credential required would be a passport or equivalent secure identification with embedded Radio Frequency Identification (RFID) that links to biometric information secured by immigration authorities. Trusted traveler enrollees' travel documents are already embedded with RFID technology and thus have the credentials already to support a biometric land exit. All other qualifying foreign nationals would register for similar credentials either in the visa, immigration benefit, or other qualified immigration setting.

For temporary visitors without a secure credential, major ports would equip inspectors with handheld or other qualified devices to gather biometrics. Technologies exist today to take a contactless fingerprint, for example, in two seconds. Iris scans are quick and reliable, and may

also be an option. However, it is recommended that this be the last phase-in of a biometric land solution when as many individuals as possible are already enrolled.

- **‘Biometric’ defined.** At land ports, the ‘biometric’ requirement for pedestrians would be modeled on the air/sea solutions. For vehicular traffic, the model would be the trusted traveler programs that employ RFID-enabled biometric verification that protects the privacy of the data by not storing private information on the travel documents, but instead linking the biometric to government-stored data. This way, CBP could still check the stored biometric (likely facial recognition) with the individual, if necessary.
- **‘Exit’ data captured.** The system would link the reading of the RFID at a land port of entry to the Arrival/Departure Information System.
- **Funding.** Four potential mechanisms, in combination or alone, are available to pay for a land border biometric exit without requiring significant direct appropriations. These include: (1) fees for the improved travel documents, based on the five trusted traveler program models that exist today; (2) increase in ESTA fees; (3) increase in visa fees; (4) local monies, both private and public to fill in the infrastructure gaps. These gaps include adding the RFID technology already employed in entry lanes at the 39 busiest land ports to the exit lanes in a phased-in approach.

Why Land Borders

Biometrics at land borders have been dogged with policy issues regarding feasibility, trumping the basic fact that most border traffic is across land, not air/sea. In addition, if the Senate immigration reform bill (S. 744) amnesty is passed, border crossing numbers are likely to rise. Even without new immigration legislation, no exit system can be complete without inclusion of land borders. Most important, three laws specifically require biometric exit to have been implemented years ago.

In regard to *why* biometric at land borders, please see prior policy discussions in the air/sea exit portion of this testimony. The value of biometrics in borders does not change per the locale it is obtained; assuring that a person’s identity is accurately recorded for departure is equally important whether departing by sea, air or land. However, because of the variety of departures at land borders, it is worthwhile to include more specificity of the unique attributes of pedestrian and vehicular crossings on the border.

- **Pedestrian crossers.** If S. 744 were passed by this body, it provides for the provisional legal status of agricultural (blue card) and low skilled workers in a new W program (eliminating H2-A). The new program caps low skilled workers at 200,000 but is unlimited for spouses and children of W applicants, which will likely at least double the numbers of those entering through land ports under the new S. 744 W program. The W agricultural workers are capped at 112,333. However, the Secretary of Agriculture may adjust the cap higher without limitation. Past estimates for agricultural workers is that 90 percent of these individuals use the land ports

for entry/exit. The same is the case with the H2-B (low skill) program, whose current cap is 66,000.

A biometric exit is absolutely essential when the numbers are this high, and have unlimited growth potential, to quickly and with assurance know who is crossing the border, and whether these individuals are abiding by the terms of their visas.

- **Vehicular traffic.** There are five trusted traveler systems currently in place that deal with vehicular traffic in a manner that is fast, accurate, easy to deploy and cost-effective. mimicking these programs for exit control could solve a significant portion of the current land border conundrum.

The idea is relatively simple:

- Turn the ‘biometric’ requirement of the eight varying ‘exit’ statutes from requiring a cadre of inspectors using handheld devices at brand new border gates for exit, to one housed in travel documents carried by legal immigrants (travel card) and foreign visitors (visa), eliminating many of the infrastructure issues that has crippled the discussion of a solution for years.
- Use the ‘biometric’ element already used for U.S. citizens in trusted traveler systems, and apply those same biometric standards to travel documents for foreign visitors and legal immigrants.
- Use the RFID technology already used for trusted traveler systems at 39 land ports of entry.
- A biometric exit-tracking system for foreign nationals departing by *pedestrians* at land ports of entry is likely feasible immediately at a reasonable cost, mimicking processing at air/sea ports of entry using interior locations at ports of entry.
- A biometric exit is feasible in the near future for *individuals and truckers already enrolled in trusted traveler systems* with little port infrastructure change and little cost. A straightforward solution duplicates the trusted traveler RFID technology used at entry lanes to exit lanes. No new IDs would require to be issued to these individuals.
- The backbone of the solution for *vehicular traffic* would be trusted traveler RFID technology that exists at entry replicated in exit lanes, and “smart cards” that mimic the technologies, security and privacy features of trusted traveler documents.
- RFID and corresponding ID card technologies are proven, cost-effective and significantly better and relatively inexpensive.
- Inclusion biometric element to the land border exit solution was proven in a January 2005 [“US-VISIT Increment 2C RFID Feasibility Study Final Report”](#) which found that using RFID technology such as that already successfully used for DHS vehicular trusted traveler programs SENTRI (southern border), NEXUS (northern border) and FAST (shippers on

both borders) could be used for exit solutions at moderate rates of speed, and different types of IDs did not disrupt collection of information.

- The difference with a biometric exit solution and today's trusted traveler systems is that the verified departure data would be recorded and then relayed to Arrival/Departure and Advanced Passenger Information Systems.
- Using trusted traveler systems as a base model for biometric exit, the essential trade, facilitation and departure collection goals of border controls can be met, including incorporating in the good work of DHS and Canada in their shared entry/exit information system and other cooperative border agreements that are maturing today rapidly and well.
- For all foreign nationals seeking entry into the United States not currently enrolled in trusted traveler programs, the U.S. should consider expanding the RFID / secure identity electronic framework into issuance of visas, border crossing cards, and other travel documents accepted to use for entry/exit across U.S. borders.
- According to the Smart Card Alliance, chips holding biometrics and RFID capable cost only a few dollars a piece.
- Cost for travel documents enhanced with biometrics and RFID capable could be folded into visa and other program fees.

Satisfying Statutory Requirements

Current law requires a biometric exit established at land ports of entry. Practicality requires, to the extent possible, that the statutory requirements be cost-effective and budget-neutral; provide accurate data; and support trade and tourism.

‘Biometric’ legal requirement satisfied. The digital photo and fingerprints already taken for the purposes of obtaining a visa or, in some cases, acquiring an immigration benefit, could be the same biometric required for the travel document, pointing back to either (1) for foreign visitors who received a visa, to the State Department's consular database; or (2) for legal immigrants, to the USCIS database. The hardware and software should be multi-modal, meaning that while photo and fingerprints are standard, iris scans, now used by the State Department and our military, for example, may be incorporated into functionality if need be in the future.

The applicant identity information would not be stored on the travel document itself, but would only be available to verify the cardholder's identity as having exited the country. The ‘biometric’ requirement of the law would be satisfied.

‘Exit’ legal requirement satisfied. The identity information of the foreign national, once verified against biographic information automatically associated with that identity, would in real time be recorded in the Arrival Departure Information System (ADIS). The ‘exit’ requirement of the law would be satisfied.

Use of land port existing technologies. For vehicular traffic where the occupants have been issued secure travel authorization documents, the program would work very much like the trusted traveler systems on the land border work today:

- When a vehicle approaches the border, all occupants present their secure travel authorization document.
- The RFID cards contain a file number that is read upon arrival.
- The file number triggers the participant's data that is available to be brought up on the CBP Officer's screen.
- If there is reason for concern, the data is verified by the CBP Officer and the traveler is released or referred for additional inspections if proper documentation is unavailable.

Use of proven travel document technologies. The proposal uses as its core the proven trusted traveler programs that currently use relevant background check vetting, CBP access to data, and RFID technologies embedded in travel documents. This proposal piggybacks on the five trusted traveler programs now offered for land port entry.

The descriptions below are examples only, and those for US citizens below, would not be necessary or available for foreign nationals.

-For U.S. citizens pursuant to the Western Hemisphere Travel Initiative. Alternatives to a passport for U.S. citizens include PASS Cards issued by the State Department and Enhanced Driver Licenses (EDLs) issued by certain northern states. Both began availability in 2009, with states like Minnesota only issuing EDLs in the past few months.

- *PASS Cards:* The [PASS Card](#) is a limited use passport in a "wallet size" format used for land and sea port entry, and only available to U.S. citizens. This ID establishes both the identity and nationality of the bearer. This ID satisfies the 9/11 Commission recommendation that became the Western Hemisphere Travel Initiative, requiring all those seeking entry into the U.S. to present a passport or equivalent. It is used by business travelers and other individuals who live in border communities as well as those that travel frequently (by land or sea) between the United States and Canada / Mexico.
- *Enhanced Driver Licenses:* State-issued enhanced drivers licenses (EDLs) provide proof of identity and U.S. citizenship, are issued in a secure process, and include technology that makes travel easier. They provide travelers with a low-cost, convenient alternative for entering the United States from Canada, Mexico or the Caribbean through a land or sea port of entry, in addition to serving as a permit to drive. Michigan, Minnesota, New York, Vermont and Washington are issuing enhanced drivers licenses.

-For U.S. citizens and qualifying foreign nationals:

Those foreign nationals enrolled in the following trusted traveler programs would be the easiest to apply a biometric exit requirement.

- *FAST*: Available to U.S., Canadian, and Mexican low risk truck drivers whose personal record and driving record are subject to numerous criminal, immigration and driving background checks, enabling use of dedicated driving lanes and faster inspection. Available at 17 northern and 17 southern ports of entry.
- *Nexus*: Available to U.S. and Canadian low risk travelers, NEXUS members now have crossing privileges at air, land, and marine ports of entry. Under the Western Hemisphere Travel Initiative, the NEXUS card has been approved as an alternative to the passport for air, land, and sea travel into the United States for US and Canadian citizens. The program allows pre-screened travelers expedited processing by United States and Canadian officials at dedicated processing lanes at designated northern border ports of entry, at NEXUS kiosks at Canadian Preclearance airports, and at marine reporting locations. Approved applicants are issued a photo-identification, proximity Radio Frequency Identification (RFID) card.
- *Sentri*: Available only on the southern border, SENTRI provides expedited CBP processing for pre-approved, low-risk travelers. Applicants must voluntarily undergo a thorough biographical background check against criminal, law enforcement, customs, immigration, and terrorist indices; a 10-fingerprint law enforcement check; and a personal interview with a CBP Officer.

Qualifying travel documents. All of the applicant data is stored in the secure USCIS database, or for the case of nonimmigrant visa holders, the State Department. No private biometric information is stored on the travel document, and thus no private information is transmitted with the RFID (RFID technology has the potential to track an individual's movements, create a profile of an individual's habits, and allow for secondary uses of that information). All applicants would already have undergone background checks pursuant to receiving the relevant immigration benefit. This solution is that used in trusted traveler systems, and has worked to protect private information.

- ***Enhanced visa page for foreign visitors:*** The current visa issued by the State Department and used for presentation for entry at U.S. ports of entry by foreign nationals in their passports would receive the enhanced travel document described above.
- ***Enhanced travel authorization ID card:*** Current and future eligible legal immigrants would receive the enhanced travel document described above.

Exit data and overstay data produced real time at land ports. The proposal would generate real time, immediate exit data at land ports, minimizing overstay data manually produced by ICE today by generating an exit record in the Arrival/Departure Information System for every exit instance. The same could be done for land port entries, building on the biographic data being gathered today on the northern border in cooperation with Canada. Current legal mandates for a biometric exit would be satisfied. Overstay data used for the Visa Waiver program and immigration enforcement generated with significantly less manual labor. National security would be better served, knowing whether a wanted terrorist or felon is in or out of the country would no longer be a guessing game, and enabling law enforcement to make better decisions about whether to rendition a wanted individual.

Privacy and security of data. The foreign national's data is kept private because it is not stored on the card, but in USCIS or State Department secure database. Instead, the card includes a file number which points to a file number in a secure DHS (immigrant) or State (nonimmigrant) database that is read upon arrival. This number does not contain any personally identifiable information.

The file number triggers the participant's data to be brought up on the CBP Officer's screen. The data is verified by the CBP Officer and the traveler is released or referred for additional inspections. This is exactly how current land border trusted traveler systems work. These cards are provided a shielded sleeve that prevents anyone from reading the document.

Minimizing cost.

- The proposal requires a phased-in RFID add-on dedicated exit lane by dedicated exit lane approach. The only new infrastructure likely required is duplicating RFID into exit lanes and technology to record corresponding data.
- Phasing in RFID technology at the ports would mirror (with planning), the phased-in approach of embedding the improved travel documents with the RFID technology in order to avoid any potential negative repercussions for trade and tourism.
- The travel document and biometric R&D is already established, and would be incorporated into the improved travel documents. Any new costs in embedding RFID technologies or biometrics could be covered by fees. Business models already exist for the travel documents mentioned above, and could be replicated in part by this program.
- The new element-- linking the Arrival / Departure Information System to the improved secure credentials-- would be minimal relative to the cost barriers of deploying fingerprint readers or other handheld technologies at the ports for all those exiting; instead, handheld devices would be the exception, not the norm.

Differentiating between US citizens, legal immigrants and visitors. To be clear, the proposed entry / exit system would not apply to U.S. citizens, only foreign nationals. In delineating between foreign nationals and US citizens, it would be efficient and useful to build upon the culling process already created by the US and Canada for their shared entry/exit biographic exit deployment.

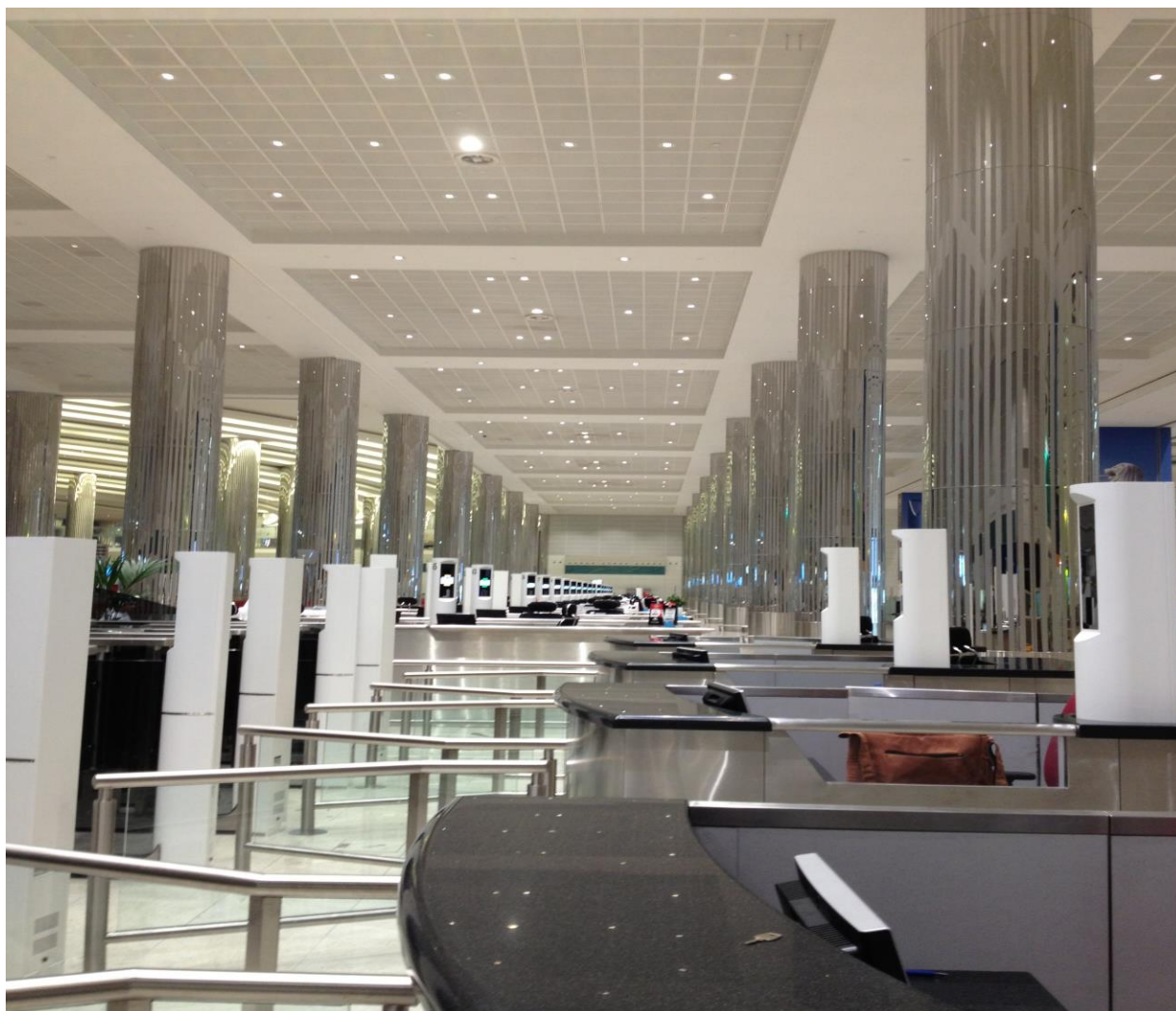
Phase-in of program. In the first years of the program, until all visas were expired and included the enhancements necessary for recording exit data, and all aliens received similar enhancements to their ID cards, the exit data would be necessarily incomplete. As travel documents expire and are renewed, these would contain the RFID-enabled / machine readable technology. The gathering of exit data would be robust.

Canada. DHS is working with Canada currently on a mutual entry/exit system at land ports (discussed above) as well as enhanced drivers licenses as an alternative to the Canadian passport. Four Canadian provinces (British Columbia, Manitoba, Ontario, and Quebec) are issuing EDLs to Canadian citizens. Canadian citizens can present an EDL when entering the

United States from Canada, Mexico, or the Caribbean through a land or sea port of entry. It would be worth engaging the Canadians on incorporating EDL linkages to the Arrival/Departure Information System, ADIS.

**BIOMETRIC SOLUTIONS AT AIR, LAND AND SEA PORTS
IN THE UNITED ARAB EMIRATES**
provided by California-based AOptix (iris recognition)

BIOMETRIC ENTRY, DUBAI UAE



BIOMETRIC IRIS-FACE Recognition, Dubai International Terminal 3

Over 100 lanes of either immigration stations or automated border control gates (even suitable for use by disabled passengers in wheelchairs) have been in place in DXB's largest terminal since early 2013. The airport is slated to see major increases in traffic and envisions iris recognition as the principal means of authenticating visitors to and transit passengers in the Emirates in one of the fastest growing transport hubs in the world. Since the implementation of 100 gates in terminal 3 earlier this year, additional systems have been ordered for deployment in terminals 1 and 2 as well as in the new Maktoum Airport just outside Dubai en route to Abu Dhabi.

BIOMETRIC TRAVEL CONTROL, IRIS RECOGNITION



Gatwick Airport, London UK

Over 25 lanes of AOptix InSight Iris Recognition are deployed at Gatwick in what is called a “mixed use departure area”-- where international and domestic-destined passengers utilize the same retail and restaurant amenities. Passenger mixing that without proper safeguards, might yield boarding pass swapping and an “Immigration Bypass” has been negated by use of an iris system that requires iris template-barcode linkage on boarding passes for domestically-enrolled passengers (no iris enrollment on the sterile side of the border). Operation of the technology is simple: instruction for self-enrollment is delivered via exposure to 2 exposures to picture-only LCD's on the domestic side. The process is simple enough that even a child can do it.

Courtesy AOptix Technologies

QATAR BIOMETRIC ENTRY/EXIT, ALL POINTS ENTRY LAND, AIR, & SEA



In an installation that dates to 2011, every point of entry into the State of Qatar relies on an AOptix Technologies InSight™ system for a black-list determination- enabled Entry/Exit program at every point of entry (80+ lanes air, land, and sea) in the gas-rich state. Every person entering and leaving the state uses the system. Notice that unlike standard white livery seen at Dubai, Qatar actually asked for sheathing that matched the color scheme of the immigration booths. More importantly, processing time for individuals with 2-eye recognition is less than 5 seconds per person.

Courtesy: AOptix Technologies