Testimony before the
Senate Homeland Security &
Governmental Affairs Committee

SECURING OUR BORDER: Biometric Entry and Exit at our Ports of Entry

Tuesday, April 28, 2015, 2:30 pm, SD-342 (Dirksen)

Janice Kephart

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

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

Executive Director of the Airport Entry and Exit Working Group, an industry group that welcomes all members of the identity management, biometric and document authentication industry that support a fast, efficient, and compliant biometric entry re-engineering and exit implementation and founder and CEO of the Secure Identity & Biometrics Association (SIBA)

North Americas Director, BORDERPOL, an international non-profit organization working on behalf of border agencies worldwide for faster, safer and more secure borders

Chairman Johnson, Ranking Member Carper, and esteemed Members of this Committee, thank you for the opportunity to testify on the implementation of a biometric immigration exit system. Creating a feasible and cost-effective solution for foreign visitors has emerged as the linchpin in fully implementing the eight statutes first passed 18 years ago. As you are well aware, the *The Final Report of the National Commission on Terrorist Acts Upon the United States* (the *9/11 Final Report*) and my team's attending monograph, *9/11 and Terrorist Travel*, providing the factual and policy backdrop for the 2004 Intelligence Reform Act that first required a fully automated biometric entry and exit system at all ports of entry. Today I testify from my base as a former 9/11 Commission staffer, with my subsequent research and work over the past 11 years continuing to buttress the recommendations found in the *9/11 Final Report*.

Tracking the arrival and departure of foreign visitors to the United States is an essential part of immigration control, 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 definitively whether travelers have left when they were supposed to. Biometric entry/exit and transfer solutions are proven in their feasibility, low cost, added security value, increased efficiencies, travel convenience, and accuracy. Good products are available off the shelf. They are flexible and built, and can be customized, for many environments. The biometric, secure document and identity management industry is well-versed in integration with back-end data systems while building in flexibility for the future. Biometric solutions such as facial recognition, fingerprints and iris scans assure identity when coupled with biographic information found in travel documents. Using *only* biographic information, however, such as names or passport numbers, provides no assurance that the person departing is the one whose original arrival was recorded.

The United Nations World Tourism Organization states that nearly 1 billion people annually are crossing international borders, or one in seven people. The only truly distinguishing feature amongst every single person? Physical identifiers, known as biometrics. Documents are designed to be replicated by governments and authorized agencies. Keeping them secure is essential, but difficult. Having biographic information for each individual is also essential. However, biographic information stored on a replicable document such as a passport, is well known to be subject to fraud and counterfeiting. However, when a biometric is added to the biographic border process - or more than one biometric for full robust security - than the ability of a fake or manipulated real passport to successfully pass through a port of entry undetected becomes extremely difficult.

While a person may try to lie with his words and his travel document, a person's physiological characteristics cannot be lost, forgotten, stolen, or forged. When truth and lies mix in this environment, truth is much more likely to win. When that truth is against a terrorist, then security wins and maybe even lives are saved. If biometric entry/exit had been in place on 9/11, it is possible that heinous act may have been prevented. However, there was no good excuse why a biometric entry/exit system was not in place when Tamerlan Tsarnaev was planning his

attack on the Boston Marathon in early 2013, and traveling to Chechnya for training immediately prior to that.

Much of the world understands the value of a Biographic + Biometric Border System. More than 80 countries now have ePassports whose embedded chips contain information that replicate the MRZ on the passport and add in at least a photo that can be retrieved using facial recognition software. Some countries are also adding in fingerprints to the chips. While ePassports are flourishing, the world is catching up with actually reading these chips to enhance security. The United States still does not systematically read the chips.

In addition to retrieving the biometric information a country stores on a chip in compliance with United Nations protocols, at least 32 countries have biometric entry or entry/exit border control. Most of these are at airports, but countries like Hong Kong have integrated biometrics into all their ports of entry including land, rail, sea and air, and the European Union is now undergoing a pilot to test a large variety of biometric border controls at all types of ports of entry as well that covers the entire Schengen area of 26 countries. Schengen permits free movement of citizens within the area, but the January terror attack in Paris has highlighted the vulnerabilities of not having biometrics at its borders to verify identity.

By way of example, one of the largest airports in the world, Schiphol Airport in Amsterdam, responsible for annually processing 55 million passengers (our top five busiest US airports add up to only 50 million international passengers a year) with 80 percent of them international transfers, is just now completing a five year build-out of 80 e-gates. The cost for this project? A mere 30 million Euros (which includes five years of maintenance and upgrades), indicating a significant downward trend in implementation costs. (Very different than the official $3 billion price tag the US government placed on implementation at international airports, and potentially even less than I projected in 2013 of about $500 million.) In addition, these solutions do more than what US immigration processes currently systematically do or, as of now, plan to do: these e-gates not only take a biometric, but assure that the traveler is the legitimate holder of the passport by reading the ePassport chip and using facial recognition software to match the individual to the stored photo.

The Schiphol processing does both in about 20 seconds on average per passenger (most take 10-15 seconds). The trend is for even faster processing. New emerging technologies are able to process fingerprints in a completely contactless, more hygienic manner, at one individual in less than a second. This is faster than a traveler can likely move! Such a solution is being tested in the European Union right now.

Findings relating to Air v. Land Biometric Exit Deployment

Today's testimony is based in part on a September 2013 60-page published report on the cost and feasibility of an **air and sea** biometric exit implementation. That report became the basis for

testimony before the House Judiciary Committee in November 2013 that provided an in-depth review of cost, feasibility, statutory requirements, program history, and worldwide deployment of biometric entry-exit systems to date. These issues are referenced here, but will not be repeated in this testimony but for necessary updates or summaries.

This testimony found that in regard to implementing biometric exit at air and sea ports of entry:

• The first-year implementation costs for all air and sea ports would range from $400 million to $600 million. This cost includes a 50 percent "overrun" risk factor of $125 million and is based on 2013 industry device costs and a 2008 Department of Homeland Security (DHS) regulatory assessment of costs associated with deploying biometric exit to all international air and sea ports, which at the time was defined as 73 largest international airports and 33 seaports.

• 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.

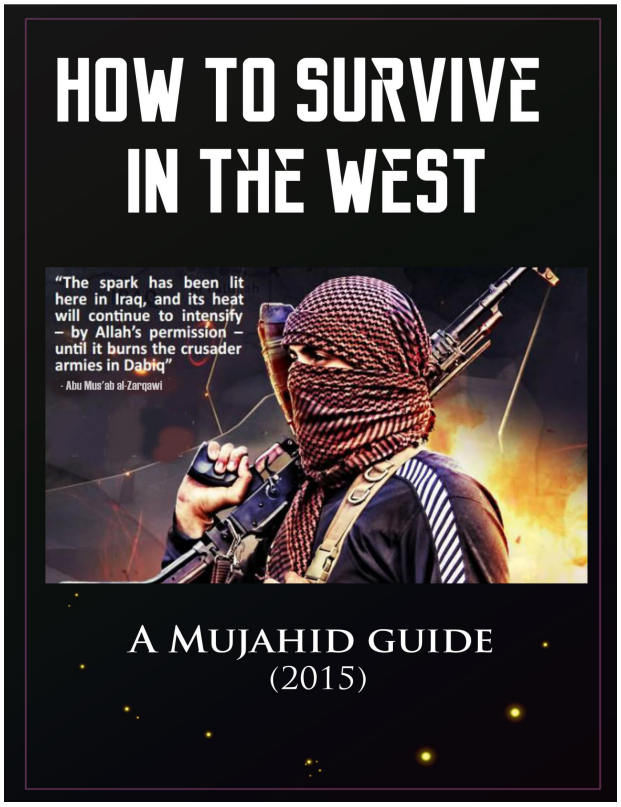
• Today, at least 32 nations already have, or are in the process of implementing, biometric processing of foreign air travelers including small countries such as Bulgaria and Ghana, while New Zealand has combined airline check-in and check-out with immigration control in its second generation system. The UAE and Hong Kong have had no issues with its biometric border control at all land, air and sea ports since installation. Hong Kong's busiest land border Lo Wu terminal handled up to 290,000 passengers a day or 92 million in 2013 alone using a passport reader and biometric e-gate style system. 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 US to New York JFK's annual processing of 12 million. As mentioned, Schiphol airport processes over 55 million international passengers a year with arrival/departure/transfer gates. 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.

• Today, DHS is conducting extensive testing by the DHS Science & Technology Directorate's Air Entry and Exit Re-engineering Program (DHS AEER) at the behest of Customs and Border Protection (CBP), with a heavy focus on biometric usability and traveler interaction.

In regard to implementing biometric exit at land ports of entry, my House Judiciary 2013 testimony concluded that the focus for implementation should be on 39 busiest **land** ports representing 95 percent of the total northern and southern border traffic. 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.

Tracking the departure of visitors leaving by vehicle by land is a very different challenge because of completely different conditions at land ports of entry versus air/sea ports of entry. However, Hong Kong has used a combination of registered traveler programs, smart cards, biometrics and travel documents as a base for their integrated border system for both those arriving by vehicles, and those on foot and is worth study here as well for applicability. That system boasts an average processing time of 30 minutes or less for entry, significantly less than the waits at US land ports. 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.



The (Again) Rising Tide of Jihadi Extremism Threatening Homeland Security, and Manipulation of Identity a Key Element of ISIS Strategy

As ISIS expands its brand of terror and widens its net with its worldwide call for other terrorists to join them, there has been a rapid rise of the need for fighters to use fake passports to get out of their home countries undetected, travel into Syria, and then back out (if they survive) undetected to their designated locations. Fake passports, aliases, and bypassing border checkpoints are critical to success. Curtailing this terrorist travel is critical to stopping this rising tide and spread of terror.[1]

Countries like Australia and the United Kingdom

[1] BORDERPOL is holding an international security meeting in Washington D.C. Sept. 9-11, "Curtailing Terrorist Travel". The website is borderpolamericas.com

are placing stringent requirements or outright banning the return or exit of such fighters. Many of these governments have identified biometric technology as a viable technology to more accurately identify travelers and help stop the spread of terrorism.

On March 28, 2015, ISIS published its *How to Survive in the West 2015* guide for ISIS recruits and members. Divided into chapters, its English translation [without grammatical corrections] begins with a section on the importance of changing and maintaining different personas depending on the audience. [I am happy to provide a copy of the guide to the Committee, as there is no link to provide.] The section below is actually broken out in blue and red to highlight its importance as follows:

> Changing your identity is important because you will come across different people in this struggle...
>
> Identity change is so important that everything about you – your: (Alias name, Physical look, Voice, Meeting places, and even phone number.) are different to your real ones. This makes it extremely difficult for intelligence agencies to know who you really are if you always take security precautions before every meeting. If you can find people who can fake ID cards, that would be even better (and this may be possible if you can have contact with people in the dark underworld)."

These types of publications are proliferating on the dark net and intercepted by intelligence authorities. These documents are not necessarily classified. (These examples are not). For example, ISIS also just published a 70-page manual in fluent English instructing ISIS members on how to best to befriend, rob, and kill from the inside of western society. The manual, according to an April 20, 2015 summary, begins with how to use online scams to steal money and raise funds, make bombs from household items, praises the Tsarnaev brothers for using a pressure cooker as their mode of attack, and then lays out how to conceal one's identity.

> Along with funds and weapons, one last aspect the guide teaches is the methods of covert operation needed to keep the terrorist attack secret and launch it without attracting attention. The guide instructs terrorists not to wear Islamic clothing, **to take on a westernized name** [emphasis added], and wear colored contact lenses to confuse witnesses. As part of the covert tactics to cover up the acts of terror, the guide's section on "secret white converts" explains how to manipulate Westerners to use them for alibis, and how to influence people in power.
>
> "Befriend good decent white people who are dissatisfied with their governments, be close to them and offer them support and guidance in life," it suggests. "If these people open up to you, you can decide if you want to tell them about Islam. You will tell them enough information to satisfy what service you require off them, but not more than that."

It is clear that an essential element of a successful terrorist portfolio, according to ISIS, is the ability to manipulate identity. Using fake IDs and taking on a different name while infiltrating western society to pretend to be a different individual, or with different intentions, is essential. ISIS is so well aware of the issue of identity and fraud that it has begun issuing its own ID cards

to prevent its own "caliphate citizens" from using the fraud they advocate to manipulate the rest of the world. The images here were tweeted on April 17, 2015. According to Australian reporting, the IDs contain a "three-dimensional chip and anti-counterfeiting hologram and are being distributed among people living in IS controlled territories throughout Iraq and Syria."

Both National Counterterrorism Director Nicholas Rasmussen and the Michel Coulombe, director of the Canadian Security Intelligence Service (CSIS), have made public in recent weeks that the number of those leaving for ISIS in Syria and Iraq, while still in the hundreds, is increasing. Those returning pose a direct threat to homeland security. Having accurate data on who is coming and going - not who is *pretending* to be coming and going - is essential to curtailing the insidious and increasing direct threat that ISIS is loudly declaring at our homeland.

As we know from 9/11, the terrorist threat may or may not be defined from the numbers of terrorists identified. A much greater concern is the training, intent and ability of those that have managed to slip through our borders undetected. Using available, efficient and accurate biometric technologies that verify both the document and its holder as legitimate, is essential. Knowing for sure they are leaving is essential to either an intelligence operation or law enforcement action. Without the biometric, a terrorist who has followed the ISIS guides and poses as an American, visa waiver country national, visa holder may succeed in bypassing our borders.

Coulombe stated on April 21, 2105 before a Canadian Parliament hearing that "the overall number [of ISIS recruits exiting Canada] is (slowly increasing), with a sharper increase with regard to Iraq and Syria. In fact in the last three, four months we probably have seen an increase of about 50 per cent in the number of people who have left for Iraq and Syria."

From a national security standpoint, the US failure to take substantial measures against ISIS, al Qaeda, or any other terrorist organization's overt strategy to use covert identities to bypass borders and embed in the United States using any name or false document is a failure of national security. Not knowing how many have left is inexcusable if they are otherwise watchlisted. As

one senior member of the our federal law enforcement community stated to me recently, having worked in identity intelligence for years, it is his experience that "biographic information lies, biometrics do not." To be clear, any implementation of an comprehensive biometric exit solution or re-engineering of biometric entry will be incomplete without:

(1) real time connectivity and matching within the foreign national fingerprint database known as IDENT, currently housed as the foundation to the Office of Biometric Identity Management's enterprise solutions that serves the intelligence and law enforcement needs across the United States, and our overseas partners;
(2) real time connectivity to relevant watch lists honed by the Terrorist Screening Center;
(3) document authentication technologies to assure the legitimacy of the passport;
(4) biometric technologies that (a) assure that the passport legitimately belongs to the passport holder and (b) quickly and accurately enroll a foreign national at entry and/or verifies the individual as the same person who entered with that passport.

Biographic Only vs. Biometric Plus Biographic

There continues to be a debate over whether a "biographic-only" approach to exit is sufficient. 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. While that particular problem has been fixed, 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 at least one of the biometrics obtained at entry (which in the United States is a digital photo and 10 fingerprints) are capable of occurring in 10-20 seconds. Departure requires only verification against one of these biometrics, face or fingerprints, or another biometric such as iris - as long as iris is engineering into entry processing.

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. It can be configured anyway that CBP would like it, using the backend of the Office of Biometric Identity Management's (OBIM) core database, IDENT, for both matching, organization and storage.

This does not mean that "hits" will result in a denial of departure or secondary inspection. In fact, that may or may not be decided to be part 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 or security risk.

Focus on High-Risk Passengers with Better Information. In 2008, US-VISIT (now OBIM) 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 Biographic + Biometric was a far better choice than a biographic-only exit 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."

To be clear, the current biographic system in place at US airports and US-Canadian biographic information sharing on cross-border traffic has continued to undergo significant improvements over the years. However, those improvements can never replace the efficiency, accuracy and speed that biometric solutions provide to assure that people seeking entry or exit from the United States are who they say they are, and/or not associated with nefarious information. Are name-based algorithms enough? Are readers that do not determine the legitimacy of the passport enough? Is not verifying and enrolled the actual physical identity of an individual enough? Not to a good counterfeiter. Not to a determined terrorist.

While our current entry processes are solid in regard to assuring enrollment or verification of already enrolled identity at our air ports of entry, these systems still fail to determine whether the biographic name provided is legitimate because the passports are not verified as belonging to the passport holder even when possible to do so. For those presenting ICAO-compliant passports that contain a chip in them that replicates the biographic and biometric information presented when applying for the passport, our immigration officers today are not systematically reading those chips, enabling counterfeit passports to still slip through. Yet these chips, with biometrics, can be the essential deal breaker for terrorists and anyone else seeking to conceal their identity when entering or departing the United States.

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. 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. The key elements

of a practical biometric exit program are reasonable, real cost estimates; tested and mission-capable technologies; usability; speed of the entire exit process per individual; and, in order to drive government accountability and long-term efficiencies in deployment, assurance that only immigration authorities, or those deputized as immigration authority, will implement and collect the departing aliens' biometric information.

Biometric Exit Data Multiplies Information for IDENT Partners, Increasing the Enterprise Value of the Office of Identity Management's Biometric Products. 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 be used by federal or state law enforcement or the intelligence community to 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. It was also a key issue in the FBI's failure to know that Boston Marathon bomber Tamalin Tsarnaev had departed for the former Soviet Union, or take seriously the warnings provided by the Russians about Tsarnaev's terrorist leanings.

As an aside, it is imperative that the Senate not approve the move of OBIM — a move being strongly considered by DHS management — to CBP. OBIM is a core cybersecurity function that belongs in the National Protection and Programs Directorate (NPPD), engineering the storage and protection of highly sensitive identity data that is critical to US homeland cybersecurity functions. OBIM's mission goes right to the heart of the NPPD mission: securing the identity of millions of foreign nationals, many of whom reside in the US. In addition, the absorption by CBP of OBIM would permanently remove the independence of the enterprise and its respective clients. More specifically, accurate and real-time exit data supports OBIM authorized law enforcement, immigration, and national security government clients. Moving OBIM to CBP places both client relationships and an OBIM budget line in jeopardy, subject to both the political and budgetary constraints of CBP. OBIM's current clients are as follows:

- U.S. Customs and Border Protection (CBP) uses OBIM'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.

Legal and Programatic History of Biometric Exit

Statutory Mandates for a Biometric Entry/Exit System for Non-Citizens. Eight statutes with various requirements for a comprehensive immigration entry-exit system have been passed since 1996. Five of these statutes were streamlined by section 7208 of the 2004 Intelligence Reform and Terrorism Prevention Act (8 USC 1365b), which 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 2004 law required full implementation of a biometric entry-exit system at all ports of entry by December 2004 with the following stated policy goals:

The Department of Homeland Security shall operate the biometric entry and exit system for non-citizens 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 utilizing language algorithms to detect alternate names.

Section 7208(d) requires “the collection of biometric exit data for all categories of individuals who are required to provide biometric entry data (emphasis added), regardless of the port of entry where such categories of individuals entered the United States”.

Further seeking to implement core 9/11 Commission recommendations, section 7208(g) requires that entry-exit data be available electronically and used in determining immigration benefit application outcomes, including visas, work permits, immigration court cases and investigations. In addition, as it pertains to non-citizens, “the biometric entry and exit data system shall facilitate efficient immigration benefits processing by … utilizing a biometric based identity number tied to an applicant’s biometric algorithm”.

Between 2004 and 2006, pilot programs for exit were undertaken at the request of Congress. The technology worked, but compliance rates were low; in part, because the airports were not mandated to place the biometric exit kiosks in locations that required compliance.

In 2007, the 9/11 Commission Implementation Act amended certain sections of the Immigration and Naturalization Act (8 U.S.C. 1187) pertaining to the control of foreign nationals’ travel. The law reiterated the need for exit data and required exit data collection apply to all foreign nationals entering under the Visa Waiver Program. The amendment in section 217(h) mandates that air carriers be required to "collect and electronically transmit" passenger "arrival and departure" data to "the automated entry and exit control system" developed by the federal government.

The amendment to section 217(i) mandates that “the Secretary of Homeland Security shall establish an exit system that records the departure on a flight leaving from the United States of every alien participating in the visa waiver program” that

“(1) shall--(A) match biometric information of the alien against relevant watch lists and immigration information; and

(B) compare such biometric information against manifest information collected by air carriers on passengers departing the United States to confirm such aliens have departed the United States.

In 2008, DHS established a 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, yet the regulation remains intact today.

In 2009, Congressional appropriators required two airport biometric pilot programs before appropriating further funds for exit. One pilot tested handheld biometric-biographic collection 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. 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 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.

In the 2013 Homeland Security Appropriations Act, appropriators made it clear that CBP is fully accountable for planning and deploying a biometric exit program. This was the first time that federal law clarified that CBP is responsible for implementing border inspection solutions at entry and exit.

DHS S&T Apex AEER Program Background. DHS Science & Technology Directorate (S&T), with CBP as its “client”, is currently testing, evaluating and developing a business case for appropriate, cost-effective solutions to enhance and improve air entry, and develop and deploy air exit. This effort is the DHS AEER Program.

The current biometric entry system used by CBP at over 100 US international airports is ten years old and was deployed in late 2004 in response to 9/11 Commission recommendations that “The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system”.

Foreign nationals seeking entry into the United States through airports today are subject to an inspector interview, a scan of the individual’s passport which reads the MRZ code for biographic information, an enrolled facial image, and a ten fingerprint enrollment which also checks against criminal and watch lists in real time.

There is no biometric exit system in place at this time. DHS AEER states that over 700 airports may be affected by biometric exit[2]. Right now, air exit is wholly reliant on the accuracy of passenger manifest lists provided by airlines to verify departure, and there is no opportunity to determine if an individual is who they say they are. According to DHS AEER, total international

---

[2] According to CBP’s own internal statistics, deployment to the busiest top 10 is about 50% of the foreign departing traveling public. The top 15 airports process about 75 percent of foreign national public, while the top 20 airports processes about 87 percent or so. It is unclear whether coverage of airports beyond the top 73 that US-VISIT identified in 2009 is necessary for any extensive biometric deployment. Today biometric portable “kits” are available, and that may be sufficient for many of these small airport international departures.

air passenger volume continues to increase, with a 21% increase compared to FY 09 and a projection of four to five percent annual increase over the next few years. While it is not clear how much of that increase is foreign national, as opposed to U.S. citizen, international travel, what is clear is that stress on immigration processing will continue to better facilitate travel while ensuring border security.

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 9/11Commission 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. The rising tide of ISIS reiterates these points, as discussed at the front of this testimony.

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.

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.

I do not believe DHS has provided information on how many unmatched arrival records exist today.

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.

Benefits of Biometrics for the Traveling Public. Foreign air travelers benefit from accurate data regarding their arrivals and departures because it minimizes errors that may affect future travel. Foreign travelers also benefit from biometrics because of the name/DOB match issue. For example, there are could easily be 1000 Mohamed Mohamed's with DOB 1/1/1980, and out of the 1000 only one be a terrorist. Yet, every single one of the 1000, if they travel, will have to be manually vetted and potentially be subjected to secondary inspection on account of the biographic match alone. Biometrics eliminates or at least mitigates traveler disruption and frees officers and agents to deal with other issues.

Biometric Entry/Exit 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. Biometrics are now being implemented in many international ports of entry worldwide to speed travelers through security and immigration check points. Some of these are single biometrics, while others use multimodal biometric identification systems at immigration check points and airport automated kiosks that are more resilient and trusted, while enabling immigration personnel to direct their focus on real threats versus the low-risk, everyday traveler. The solutions vary from fingerprint and facial recognition devices to iris scan technologies and more; 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.

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, like Nigeria and the Phillipines. 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, such as KLM Airlines and South African Airlines. Some of the most advanced systems, such as New Zealand's second-generation deployment, are integrating airline check-in and boarding with immigration entry/exit. And Hong Kong applies biometrics to all its ports of entry with significant success, while the European Union is committed to figuring out what biometric system works best to integrate all the Schengen border points of entry and exit.

In the United States, biometric automated passport control first was introduced at Chicago O'Hare Airport in July 2013. Today, a total of 24 airports are using the kiosks in CBP international arrival areas, all at the expense of the airports and in cooperation with CBP. JFK International Airport has experienced a wait time reduction of 66 percent, the other airports average wait time reduction is 40 percent, a significant improvement in traveler facilitation. With the exception of the US experience using kiosks at arrival, this section summarizes many of those advances.

Entry/Exit Systems by Country

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.

Angola has 10 facial recognition and fingerprint e-gates installed at Luanda Quatrol de Fevereiro Airport. In 2009, travelers reviews of Angola's airport were, in short, "horrendous"! More recent reviews read "The airport is generally well managed with efficient immigration both for arrival and departure. It took me only 5 minutes to clear immigration. … Overall a good experience." Customer Rating : 4/5 "This airport has transformed and there is now a new terminal, self check-in kiosks, computer check-in, LCD screens with flight departure information, two restaurants, and plenty of seating. While simple and basic, it is nice and clean."

Australia. With a project that began in 2004, SmartGate was the first Automatic Border Control Solution in the world to use facial recognition and e-Passports that consists of 78 e-gates and 127 kiosks to Australia's eight international airports. The solution that has been delivered consists of one advanced software system that manages all the acquisition process and the face recognition, a kiosk, and a gate.

According to the vendor, the SmartGate project was in 5 phases:

Phase 1: Installation of e-gates in two airports to prove the capability of the system to process aircrew and passengers in different locations; live facial biometrics were compared to data stored in a central database.

Phase 2: Hardware and software modifications of the e-Gates to process ICAO passports. Facial biometrics were compared to the portraits stored in the passports' contactless chips of some 6,000 selected aircrew and frequent travelers.

Phase 3: Definition of the final SmartGate solution to be deployed.

Phase 4: Full scale installation at the 8 Australian International airports.

Phase 5: Service support and continued expansion of the fleet of kiosks and e-gates.

The SmartGate solution became the foundation for e-gate solutions that are now deployed by various vendors across the globe and involves two steps: passengers first place e-passports on a scanner at a kiosk, which unlocks and reads data stored on the chip embedded in the e-passport. After answering standard declarations, such as where the traveller has been, a ticket is issued. The passenger then proceeds to a biometric gate equipped with face recognition cameras where data associated with the ticket is cross-checked against biometric data collected from the person. The system uses face recognition algorithms and technology. Gates are connected to a database server informing whether a passport holder is allowed to enter.

Originally targeting only Australian and New-Zealand e-passport holders over the age of 16, Smartgate has been widening the scope of eligible travelers since 2011. This solution, in April 2015, will be replaced at less than half the cost of the original contract with what Australia is calling “upgraded facial recognition” kiosks.

In addition, in regard to deploying exit, Australia’s decision was spurred with a convicted terrorist who had served time stole his brother’s passport and attempted to leave Australia and join ISIS in 2014. Australia’s Immigration Minister Scott Morrison stated in response to pressure to explain increased biometric border laws and deployment at departure zones “the laws were a proportionate response to combat risks posed to Australia and ensure greater monitoring of movements in and out of the country. ‘What we’re talking about here is biometric information which is becoming a common standard in what governments do to protect their citizens and to work together to protect more broadly against counter-terrorism and transnational

crime and these tools are becoming the basic tools that are really necessary in a modern age to combat the real threats in a proportionate way,' " he said.

Belgium has six e-gates using both fingerprints and facial recognition at Brussels Airport installed in 2015.

Brazil has installed 16 e-gates using facial recognition at San Paulo and Guarulhos International Airports.

Bulgaria. Bulgaria's Sofia Airport has installed four e-gates automated border clearance using both e-passports and facial recognition technologies that process passengers in 7-10 seconds. The new gates are available for Schengan and Swiss travelers over 18 years of age. Varna International also has four e-gates. 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.

On April 21, 2015, "Canadian Government announced additional financial investment for biometrics.

> Biometrics Screening
>
> Budget 2015 also highlighted the importance of biometric immigration screening as an effective means to combat identity fraud and abuse of Canada's immigration system.
>
> The CBSA will invest up to $65.8 million over the next five years to "expand the use of biometric screening to verify the identity of all visa-required travellers seeking entry to Canada." This investment will see the introduction of new kiosk technology at Canada's major airports that will enhance border management and immigration security."

Colombia. Three Colombian international airports, including Bogota, have installed finger/face e-gates as of 2012.

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.

Dubai. 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 utilizing both iris and face recognition. The airport has experienced 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, additional systems were ordered for deployment in terminals 1 and 2 as well as in the new Maktoum Airport just outside Dubai en route to Abu Dhabi.

Estonia has a two-step border control system consisting of 6 kiosks for performing customs and formalities, face matching and single-fingerprint enrollment. The fingerprint is used as a token to open e-gates at the airport exit. The system at Lennart Meri Tallinn Airport was deployed in 2012.

European Union. European Union member states are implementing pilots to test their "SMART BORDERS" strategy aimed at creating a comprehensive Entry and Exit system for processing TCN (Third Country National) travelers and an RTP (Registered Traveler Program) for TCNs. (All EU systems currently do conduct document authentication.) The concept includes self-service border control using automated border control gates at air, land, rail and sea ports that incorporate facial recognition and now fingerprint verification as well, while running against e-passport data for verifying the passport belongs to the passenger. Right now, the system is optional, and travelers may still be processed by immigration officers, although the plan is for full automation.

According to recent news reports, a draft internal EU document dated February 18, 2015 "lists Arlanda (Sweden), Charles de Gaulle (France), Frankfurt (Germany), Lisbon (Portugal), Madrid (Spain), and Schiphol (Netherlands) as participating airports. Frankfurt and Schiphol will ask between four to ten fingerprint sets. Madrid will ask for four and Charles de Gaulle eight.

"Arlanda, Charles de Gaulle, and Madrid airports are also set to start requesting facial image-captures from disembarking passengers. The airport in Lisbon is ticked to perform iris pattern scans but the paper notes that "iris pattern of volunteering TCNs [third country nationals] should be captured live, at the same time as the facial image.

“The biometric screening extends to road, train, and sea routes as well and includes iris pattern scans in some areas. Iris scans are set to be asked on roads leading into border towns Udvar in Hungary and Sculeni in Romania. Drivers should also expect live face scans in Sculeni. Other border towns will ask for fingerprints. These include roads leading into Kipoi Evrou in Greece and Vaalimaa in Finland. At the land borders ‘the traveller will walk up to the border guard or be one of the first persons to be called by the border guard.’ Participating cars and buses will be pulled aside in a waiting area.

“Border guards will also be performing fingerprint scans on moving trains from Paris (Gare du Nord) and Lasi (Romania). Travelers at the Lasi station may also be asked for facial image captures. Seaports and moving vessels in Helsinki (Finland), Port of Piraeus (Greece), Cherbourg (France), and Genova (Italy) are also set to participate.

“eu-LISA, a EU agency tasked to manage large-scale information systems used by border guards and law enforcement, is running the pilot. It will issue the European commission a mid-term report by 15 July with a final report expected in November. The package includes the Entry/Exit System (EES) and the Registered Travelers Program (RTP). Both rely on the collection, storage, and processing of biometric data to enhance border control checks on any non-EU national entering the EU. EES is meant to identify and prevent people from overstaying their visas. Visa and non-visa holders can also get a special token under the RTP system before traveling. RTP is intended to make it easier for people like business travelers to enter and leave border gates with ease.”

Finland had 38 facial recognition e-gates installed in 2009 at Helsinki International Airport.

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 with the installation of four arrival/departure gates. The rejection rate is less than 3 percent.

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.

Hong Kong. Hong Kong has one of the most extensive, sophisticated and busiest border systems in the world. All of its entry points at air, rail, sea and land (both pedestrian and vehicular) use biometric facial recognition e-gate or mobile technologies, with emphasis across these ports of "express e-channels" that use a combination of passports, smart cards issued to residents of Hong Kong, and face recognition technology to speed travelers.

The information in this section can be found in the Hong Kong Immigration Department's 2013 Annual report. The Hong Kong International Airport (HKIA) is one of the busiest airports in the world. In 2013, 41 million landing and departing passengers used the HKIA (comparable to JFK, which has 53 million passengers handled per year). In 2013, 100 per cent of residents and 99.6 per cent of visitors were cleared within 15-minute waiting time in the Airport.

For example, in 2014, according to the Hong Kong SAR Immigration Department, Lok Ma Chau is "the busiest land boundary control point for cross boundary vehicles such as Cross

Boundary Shuttle Buses, cross boundary coaches, cross boundary goods vehicles and cross boundary private vehicles, etc… this single busiest land border entry point between China and Hong Kong processed 219 million passengers and 15.2 million vehicles [in 2013]."(Significantly greater than the US processing at the US southern border of 174.7 million).[3]

Another pedestrian land port, Lo Wu, is the "the major land boundary control point, with a purpose-built Visitor Clearance Hall. Being the busiest control point in Hong Kong with the

---

[3] US land ports of entry passenger processing:

Air	105,039,142
Northern Land Border	69,602,636
SW Land Border	174,705,373
Total	349,347,151

highest passenger traffic, the Lo Wu Control Point handled over 92.1 million passengers in 2013, with a peak daily passenger traffic of over 280,000. (This is greater than all the US northern ports of entry processing combined of 69.5 million). In 2013, using the combination of travel documents and biometrics at 25 "e-Channels" (similar to e-gates), 99.4 per cent of passengers were cleared within 30 minutes. These types of statistics are repeated throughout Hong Kong using similar technologies in all varieties of ports of entry.

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."

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 processed about 1,000 passengers per day. Authorities noted 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."

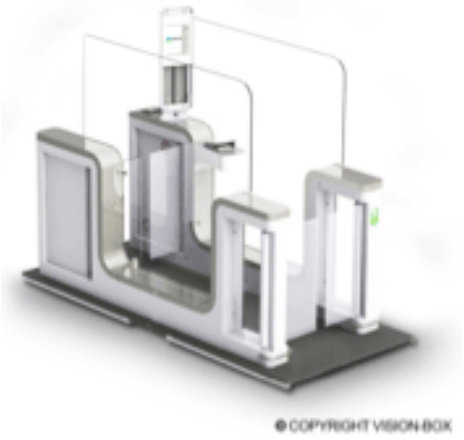
Alan Shatter, Minister for Justice, Equality and Defense, commented: "Border control arrangements at Dublin Airport are currently undergoing major change. Immigration control processes are being reviewed and leading-edge border technology such as automated gates is being tested. Many major European airports 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." Ireland has now installed at least two e-gates based on these pilots.

Japan has a fingerprint automated gate system in place for registered participants, but in August 2014 announced that in anticipation of hosting the Tokyo Olympics in 2020, Japan's Ministry of Justice will begin testing facial recognition technology for automated immigration gates with the goal of deployment by 2018. These are to be "non-stop gates" with trials at the Narita. Haneda Airport will also receive the final product. Officials have found that while the fingerprint automated gates work, the registration requirement is slowing use. According to

BiometricUpdate.com, the biometric upgrade is to employ more "rapid screening system to diminish airport crowding. The ministry's Immigration Bureau of Japan division said that the new system will analyze facial information from IC chips embedded in passports and cross-check it with pictures of passengers taken at the immigration gate.

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 world's sixth busiest 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.

According to the Schiphol Group's annual report, Amsterdam Airport Schiphol has grown into Europe's Preferred Airport, with direct connections to 319 destinations. In 2014 the number of travelers served by Schiphol grew by 4.6% to almost 55 million, with about 80 % international transfers. In the United States, our top five busiest airports combined are not as busy as Schiphzl is for international passenger processing. By way of contrast, JFK Airport is the US largest airport at almost 12.5 million international passengers annually. In 2011, Amsterdam Airport Schiphol began deploying 36 Automated Border Control (ABC) gates at Arrival, Departure and Transfer level that are flexible and able to be used for any of these processes. By the end of 2015, there will be 80 Automated Border Control gates.

The systems use facial image recognition technology along with passport readers that associate the passenger with the document, while enrolling the facial image for regulated use by border authorities. Both the airport and airlines have a stake in direct management of the technology, in a 50/50 public/private partnership between the Netherlands Justice and Defense Ministry and the Schiphol group.

The Group has even deployed an automated baggage drop system as shown above.

The airport has found a security value in the deployment with increased watch list hits and fraud determinations, and more accuracy in performing automated passport checks. Average processing time is 20 seconds per passenger, and performance is continually monitored. The cost for this substantial deployment was 30 million Euros, and that includes five years of future maintenance and upgrades. It took six months to create a solid back-end system connectivity. The biggest challenges were not the technology, but organizational changes of the new system to the airport as well as training of border control personnel.

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.

In 2012 the latest version of the SmartGate was installed. The new version 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. The solution uses "face-on- the-fly" technology. The current installation is 8 facial recognition departure e-gates, 14 arrival e-gates, 17 departure kiosks, 36 arrival kiosks. 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 is available for passengers over 16 years old carrying a New Zealand, Australian, U.S., or UK e-passport.

Norway has 16 facial recognition e-gates in three international airports, including Oslo.

Portugal has 67 facial recognition e-gates in five airports deployed in 2007.

Qatar has biometric entry and exit deployed throughout the country at all land, air and sea ports. Hamada International Airport has 64 e-gates that employ face recognition, fingerprint and iris scans as of 2014. The installations began in 2011 every point of entry into the State of Qatar relies on iris scans system for a black-list determination. Every person entering and leaving the state uses the system. Processing time for individuals with 2-eye recognition is less than 5 seconds per person.

Rwanda has two ABC face recognition e-gates at Kigali International Airport installed in 2011 and 16 gates and enrollment kiosks installed at the busy Rwanda-Congo border in 2014. The registered traveler program significantly expedites crossing of the busy land border for daily commuters..

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.

Singapore. In 2006, Singapore introduced an Enhanced Immigration Automated Clearance System for registered nationals that scans the bio page of the passport, reads the chip, then upon verification of the document information, enables the individual to scan a thumbprint that is verified against the national database.

In 2015, Singapore is testing a land border solution that employs robotic arms with biometric scanners for use by car drivers and passengers for a fast, automated clearance that also improves security, replacing inspectors. Drivers will disembark and scan all passports of vehicle's passengers, and then the biometric robotics would conduct both facial recognition and take fingerprints of the vehicle's occupants. The inspector simply verify that the processes were properly completed. The goal is to process a vehicle every two minutes.

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 uses 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 Arab Emirates. The UAE was a pioneer in deploying 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.''

United Kingdom. From 2011 through 2015, all of the United Kingdom's 12 airports will have installed over 150 facial recognition e-gates. The process began with 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 was denied boarding.

Gatwick Airport, London UK

Over 25 lanes of 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.

Venezuela has six face/finger e-gates at its Maquetia Simon Bolivar International Airport.