Testimony of

C. Stewart Verdery, Jr.

President
Monument Policy Group
January 31, 2007

Prepared Testimony by C. Stewart Verdery, Jr.
Partner and Founder, Monument Policy Group, LLC
Adjunct Fellow, Center for Strategic and International Studies
U.S. Senate Committee on the Judiciary
Subcommittee on Terrorism, Technology and Homeland Security
on "US-VISIT: Challenges and Strategies for Security the U.S. Border"

Washington, D.C.
January 31, 2007

INTRODUCTION

Chairman Feinstein and Ranking Member Cornyn, thank you for the opportunity to return to the Senate Judiciary Committee to discuss the challenges that the country faces in developing and deploying an effective mix of policy, technology, and resources to secure our borders. Not only must these programs deter and detect those who would commit acts of terrorism or crime, or violate our immigration laws, they must also welcome those who contribute to our economic livelihood and maintain our diplomatic position in the world.

I am currently a partner and founder of the consulting firm Monument Policy Group, LLC and an Adjunct Fellow at the Center for Strategic and International Studies. I also recently served as a member of the Independent Task Force on Immigration Reform and America's Future which was chaired by former Senator Spencer Abraham and former Congressman Lee Hamilton and managed by the Migration Policy Institute. 1

SUMMARY

This written testimony discusses how to build on the current success of the US-VISIT program within the Department of Homeland Security. In my view, there are six primary areas of activity that should be funded aggressively by the Congress and implemented by DHS and its partners within the u.S. government and abroad:

? Airport Exit

? International Registered Traveler

? Land Entry and Exit

? Transition from Two-Fingerprint Capture to Ten-Print

? International Cooperation

? Employment Verification

I have great faith in the US-VISIT program office and their partners in the new Office of Screening Coordination at DHS to make the best use of available resources and authorities, but their success requires a budget commitment and making tough policy decisions for imperfect operational environments.

BACKGROUND

As you know, I served as Assistant Secretary for Border and Transportation Security (BTS) Policy and Planning at DHS from 2003 through 2005. I was responsible for policy development within the BTS Directorate, working closely with Under Secretary Asa Hutchinson and Secretary Tom Ridge, in the areas of immigration and visas, transportation security, law enforcement, and cargo security. These policies largely were carried out in the field by BTS agencies such as U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and the Transportation Security Administration (TSA). BTS' functions have been subsumed and enhanced under the new DHS structure, most notably the new DHS Policy Directorate.

During my time at DHS, the department deployed revolutionary uses of biometrics to better secure our borders and transportation systems. Most famous of these success stories was the creation of the US-VISIT program. This initiative has come under sporadic criticism for not yet encompassing a 100% entry-exit system but such critiques fail to recognize the necessity of deploying US-VISIT in manageable stages to ensure success. Before Secretary Ridge and DHS took the bold step of allowing an entry-exit system to be built in increments, the United States lacked an automated entry and exit system that would allow us to know when foreign visitors arrive and when they depart for many years after it was technologically possible. Following the bombing of the first World Trade Center in 1993, Congress demanded that an entry-exit system be installed at our ports of entry, but it did not happen, and none was in place on 9/11. Remarkably, on that date the Immigration and Naturalization Service continued to rely on a paper system, and employees literally hand-keyed in departure information into a database weeks after the fact. With no exit system, and only a minimal, unreliable entry system, our entry and exit data was spotty at best, and criminals were able to come and go across our border, some of them dozens of times under different aliases, without detection. Year after year passed because nobody could figure out how to deploy a universal system all at once that would actually find terrorists, criminals and visa overstayers without crippling international trade and sparking outrage among the business persons, students, and tourists we need to attract to our country.

But in 2004, DHS rolled out the entry-exit system known as US-VISIT. We improved on the Congressional mandate by adding a biometric requirement to the system. To capture biometrics, US-VISIT electronically scans a visitor's index fingers and takes a digital photograph at a kiosk - all in the space of seconds. The biometrics captured by USVISIT allow consular and immigration officials to confidently tie travelers to the visas and passports they are carrying, and permit the development of an internationally uniform standard for identifying travelers. The unpublicized

success of the existing portions of US- VISIT sometimes makes it easy to forget how significant the achievements have been: DHS created an operational system in less than a year that launched at our air and sea ports in 2004 that now has enrolled around 80M travelers and has identified over 1800 criminals and other inadmissible persons.

Further incremental deployments continued this record of success when US-VISIT expanded to cover air travelers arriving under the Visa Waiver Program (VWP) in 2004 and persons entering at land borders with visas and under the VWP in 2004 and 2005. It is not possible to know how many terrorists or criminals have been frightened away from attempting to enter our country because of US- VISIT, but the number surely must be substantial. The 9/11 Commission took a hard look at the US-VISIT and basically said that DHS was on the right track, just to deploy the system more quickly.

Among other aspects of my work on US-VISIT, I had the privilege of chairing the federal advisory committee created under the Data Management Improvement Act, known as the DMIA Task Force. The committee advised DHS on how border enforcement regimes would affect the flow of traffic through our ports of entry and provided valuable research that is still relevant enough to be cited in the current 2006 Government Accountability Office (GAD) report under discussion today.

It is unfortunate that many other screening programs, like those designed to issue credentials to transportation workers and vetting of domestic air passengers, have floundered to date because the government could not successfully deploy an entire program at once. Those other setbacks, however, should remind us of the success of USVISIT and the wisdom of building the program in manageable steps.

However, since this initial burst of activity in 2003-2005, the program has not seen similar growth. In part this is due to the fact the program's budget has essentially been flat, between $330M and $362M a year, just enough to pay for existing operations and important interoperability work with the FBI's computer systems. In addition, the post-Ridge leadership at DHS has gone the extra mile to try to coordinate US-VISIT efforts with other credentialing and screening programs, resulting in unfortunate delays. However, with the right combination of aggressiveness and funding, 2007 could be the year when US-VISIT makes great progress in becoming the universal entry-exit system that Americans deserve and expect.

Those of us who follow US-VISIT closely were very interested to see the recent report by the GAD concerning the progress, or lack thereof, of DHS and US-VISIT to build a more robust exit capability at our land borders. One prominent news source reported it as a significant bombshell, reporting the alleged recent decision not to deploy an exit system at our land borders as a "major blow" to the Bush administration. US-VISIT apparently had taken a shocking turn away from plans to monitor the departure of Mexicans, Canadians, and others driving or walking out of the country.

Except that it is not so shocking, and not a change of plans. The executive branch has never requested, and Congress has never provided, funds to build the infrastructure and technology to track departures at the land borders. But while there was really no new news here, the press that

the "bombshell" generated hopefully will have the effect of highlighting the need to complete US-VISIT just as Congress takes up the FY08 homeland security budget.

AIRPORT EXIT

Simply put, DHS and US-VISIT must end two years of deliberation and meet the statutory mandate to build a biometrically-based exit system at air and sea ports. The controlled nature of these environments makes deployment possible without great expense. Limited pilots conducted since 2004 have educated travelers about the exit requirement. To date, however, DHS has refused to make the tough call whether to place the exit requirement at the airline check-in counter, at the TSA security checkpoint, in the secure boarding area, or at actual departure gates, or to deploy a system that combines multiple layers of confirmation. To be fair, it is true that all of the options are imperfect until we build airports with immigration departure controls, as do many other countries.

Taking the situation as it exists, and not as we might wish it, the "air exit" should be built as part of the TSA checkpoint for the following reasons:

? The TSA security presence provides a workforce used to interacting with the traveling public and able to steer foreign travelers to the exit kiosk or station;

? The checkpoint already includes technology connectivity that can allow the exit kiosk or device to receive updated watchlist information or other alerts; and

? The checkpoint is a natural "funneling" location to minimize the confusion faced by travelers and the connectivity burden that would be necessary at check-in counters or gates.

For this system to work effectively, however, air carriers will need to code boarding passes to indicate to TSA personnel which travelers require "exit." In addition, and most importantly, air carriers' departure passenger records provided to CBP will need to be matched against the biometric exit records to ensure that individuals did indeed depart the country.

Over time, it may be possible to deploy "exit" at the airline check-in counter or at the gate, but changing airline booking or check-in systems has proven a controversial, expensive, and slow process. Programs such as the pre-flight Advanced Passenger Information System (known as APIS + or as Automated Quick Query) at CBP, or Secure Flight (previously known as CAPPS II) at TSA have seen years of delay while agency personnel negotiate with air carriers and airport authorities. Relying on a proposal that requires airlines to change their reservation and/or check-in processes in all likelihood means we will not deploy an air exit system until next decade, a simply unacceptable outcome. A TSA checkpoint proposal, on the other hand, could be implemented in under a year at major airports, and at all international airports within a handful of years.

The build-out of a true air and sea "exit" system should allow the U.S. to change our visa system in several important ways. First, the overwhelming majority of potential business or tourist visitors to the United States who are refused a visa are turned down for reasons that have nothing to do with terrorism. Under U.S. immigration law, it is the burden of the would-be visitor to

convince the consular affairs officer reviewing his or her visa application that he or she does not plan to immigrate illegally to the United States. This decision cannot be appealed within the Department of State (DOS) and cannot be reviewed in any court. The overall refusal rate hovers around twenty-five percent, with rates much higher in non-Western countries. So when we hear the accurate statement that once applicants receive a visa interview about 98% receive their visa within two or three days, remember that 25% of applicants are turned down on the spot for reasons that have nothing to do with any crime or prior immigration violation they may have committed or a connection with terrorism.

Our failure to deploy any meaningful system to track whether visitors have left the country under the terms of their visa has forced us to guess ahead of time which people are likely to overstay. Imagine the United States as a business seeking "customers" from overseas to sell our products and ideals. Since we have failed to build an "exit" tracking system, we are essentially telling millions of potential "customers" that we are not willing to even allow them into our store.

The Visa Waiver Program should be altered to allow a select category of additional economically-advanced countries to enter the VWP if they meet a series of tough security measures once the air exit portion of US-VISIT is constructed. If nationals from a new VWP entrant do not compile a sterling record of on-time departures from the U.S., their participation would be suspended. Moreover, once the exit capability is in place, the participation of existing VWP countries can also be conditioned on their compliance with the 90?day stay rule. And those entering on full-fledged visas can be tracked as well. The recent expansion of the Fugitive Operations at ICE should allow for in-country enforcement of overstays who represent any particular security concern. This approach is similar to, but tougher than, that advocated by DHS, and has attracted support from the travel industry.

It is worth noting that a sea exit, largely for cruise ship passengers, is not nearly a difficult task as the air system, but needs to be constructed as well over time.

Some may argue that building an air and sea exit system is foolish until and unless there is also a land exit, especially if VWP entrants depart the U.S. by land. However, even if there is no legal or practical barrier to VWP travelers traveling to Canada or Mexico by land for short trips, we can easily require that they still depart on time via an airport as a condition of their initial entry.

INTERNATIONAL REGISTERED TRAVELER PROGRAMS

A key component of continuing to attract and facilitate travelers to the U.S. should be the aggressive construction of an international registered traveler (IRT) program. This program would build on the model of existing CBP NEXUS and SENTRI programs for land and air travel between the U.S., Canada, and Mexico and bring to life the vision of Secretary Ridge's January 2005 announcement of such a pilot operating between the Netherlands and the U.S. While it would be beneficial to travelers who undergo enhanced vetting to receive preferential treatment at a foreign departure airport, the main use of biometrics would be to exempt IRT enrollees from normal immigration and customs processing at U.S. ports of entry. Enrollees would simply have their travel documents scanned at a US-VISIT kiosk, provide fingerprints to ensure a match to the documents, and proceed to pick up their luggage. This system will require construction of real-time connectivity to the IRT kiosks.

On the front end, enrollees would need to be vetted for any connection to inadmissible behavior, including terrorism, criminal behavior or prior immigration violations. Especially for Visa Waiver Program travelers, such a review will need to be thorough and include an interview by a trained U.S. inspector. If done correctly, the program would be an excellent example of risk management to enable CBP to focus on riskier visitors. It would also send a strong signal to the customers, clients, and co-workers of the world, whose travel we need to be able to expedite, that the U.S. is open for business.

The British use of IRT is perhaps the most instructive example for the U.S. due to their understandable concerns both about foreign guests and citizens with ties to terrorism. Project IRIS is a biometric-based passenger screening system implemented in the past two years using biometric technology at Heathrow, Gatwick, Birmingham, Manchester, and Stansted airports. The British government anticipates that within five years more than a million people will be registered to use the system.

While an initial IRT program maybe open only to returning U.S. citizens and legal permanent residents, the U.S. should allow foreign travelers to enroll following an in person interview with CBP officials and a thorough background check. This interview could occur at a U.S., airport or at overseas location CBP has a presence, such as at locations with an Immigration Advisory Program. In addition, enrollees in any IRT program should also be enrolled in the TSA domestic registered traveler program as well - so that international travelers will find traveling within America convenient, especially as they move through U.S. customs processing and onto a domestic flight.

LAND ENTRY AND EXIT

Background

The next several years will see a convergence of major initiatives affecting how traffic flows across our land borders with Mexico and Canada:

? The possible deployment of US- VISIT to primary lanes of our land ports of entry and exit;

? The requirement under the Western Hemisphere Travel Initiative that U.S. citizens and Canadians present a secure travel document to enter or reenter the U.S.;

? The implementation of improvements in driver's licenses under the REAL ID law and the possibility that secure licenses might be used for border crossing purposes under WHTI; and

? The possibility of a new guest worker program to ensure that foreign workers able to pass a security check are allowed to work for willing employers in the U.S.

While it is understandable to focus on the relatively poor results of the recent land border exit pilots using radio frequency identification (RFID) technology to detect the departure of aliens holding special 1-94 forms, this test is only a small part of the larger set of issues to be addressed.

Despite the operational problems found by the GAO in the 1-94 pilots, a RFID-based system can work both in the controlled environment of an entrance port of entry and in the uncontrolled environment of a highway exiting the country.

Entry traffic lanes must be constructed or altered to allow for wireless connectivity to identify watchlist or criminal hits in time for an inspector to refer a potential entrant to secondary processing. While it may not be feasible to conduct a one-to-one check on all applicants (i.e., is the person holding the identification card the same person to whom it was issued), a one-to-many check (i.e. does the information on the card indicate a watchlist hit) should be feasible. Building a system of biometric records that can be read through a pointer system by border inspectors upon entry and by border inspectors upon departure will be costly, perhaps in the range of $1B in one-time construction costs.

However, a considerable amount of the ongoing cost should be borne by the travelers purchasing next-generation travel documents.

Western Hemisphere Travel Initiative and REAL ID

Currently, only a small fraction of cross-border travelers have RFID-equipped travel documents, but that situation is about to shift dramatically. Under the current WHTI implementation plan, DHS and the DOS announced plans to buy and distribute passport cards to millions of Americans. These IDs would look like driver's licenses. Under this plan, almost every U.S. citizen would have to either purchase a full-fledged passport ($90) or the passport card ($45) if they planned to reenter the country. These cards would be equipped with vicinity RFID to transmit a pointer to a database containing previously-supplied biographic information to allow CBP to conduct watchlist checks on individuals arriving at land ports of entry. It is further expected that Canadian provinces will build and supply a similar travel document to its citizens to facilitate their travel. After many delays throughout 2005 and 2006 and Congressional activity to allow for additional time to deploy the Passport card, the program appears on track to supply credentials later this year.

There may be another WHTI solution, however, that needs to be tested and implemented - a secure driver's license. In May 2005, Congress passed the REAL ID Act, which calls for an unprecedented reform of drivers licenses if the documents are to be used for federal purposes, such as traveling on a domestic flight. The new law requires states to scrutinize and store identity documents and to implement tight security regimes on the production of credentials, and states are also checking numerous law enforcement databases to find imposters and criminals. It is difficult to ascertain any security advantage in the vetting process to obtain a passport card versus a REAL ID license, especially since DOS will ask individuals to submit licenses as part of a passport or passport card application.

Unfortunately, there is not yet a robust federal effort to combine the programs. The DOS wants to maintain responsibility for determining citizenship, but there is no reason why the federal government cannot cooperate with states so that citizenship information could be securely conveyed for the department to decide whether an applicant is entitled to a border crossing document that the state would issue. If a state did not want to present this option to its citizens, it would not have to do so.

Washington state officials recently requested that DHS authorize a pilot project for scanning driver's licenses at the British Columbia border to test the viability of using driver's licenses rather than passports to secure border crossings. While a federal passport card may be one way to meet the legal mandate, there is no reason to deny a state the ability to provide its citizens with an equally secure, more convenient option.

States will need to recognize the technical needs of DHS and build credentials that can be read by the same federal readers while providing DHS advance information about travelers via Radio Frequency technology. WHTI was designed to simplify and speed up the border inspection process, and states should not expect that DHS will allow a plethora of acceptable cards and technologies at the border.

In addition, Congress should offer generous grants to help states implement REAL ID, which is going to cost states billions of dollars over the next decade. Even passports are insecure if source documents like drivers licenses themselves are candidates for fraud.

Border Crossing Cards

WHTI will deliver a huge amount of RFID-enabled cards to Americans and Canadians. The overwhelming majority of Mexican visitors to the U.S., however, travel with a Border Crossing Card (BCC), or Laservisa, that does not have RFID and normally is only subject to a visual comparison with the card holder at the primary inspection booth. As soon as the RFID standards are finalized for the Passport card in the ongoing rule-making at the DOS, the regulations and procurement rules governing the BCC need to amended so the BCC operates as a Passport card as well.

There will still be a significant number of travelers arriving at land ports of entry without RFID-equipped documents for the foreseeable future as legacy passports, new proximity RFID passports, and perhaps other documents are presented. However, moving a large percentage of the flow into the RFID category will keep wait times manageable and enhance security at our ports of entry.

Land Exit

It is hard to imagine that it will ever be a worthwhile investment to build a "mirror" system of controlled exit stations at an estimated cost of at least $2B complete with checkpoints and inspectors. This figure is prohibitive under any reasonable current budget scenario. Technology which is deployable during the remainder of this decade, however, should allow the construction of a system that records via RFID that a travel document has departed the country. During the next decade, a new generation of travel documents that must be activated via biometric means during the exit zone should be within reach.

A reasonable goal over the next several years is construction of a system that will inform DHS whether persons departing the U.S. have complied with the terms of their entry, with relationships built with Mexican and Canadian authorities to assist with the very rare case of a departing individual who needs to be apprehended immediately.

It is true that Congress has passed legislation which requires submission of a plan to deploy a universal biometric entry-exit system. A system that does not confirm that an individual has indeed left the country does not meet this requirement. Congress, however, cannot expect DHS and US-VISIT to build a system while not providing an adequate level of resources to do so.

According to the GAO report, only around $182M was appropriated to US-VISIT during FDY03-05 for land border operations, and that figure includes building VISIT capabilities in secondary processing for visa and Visa Waiver Program travelers. If the Congress is serious about a land exit solution, the budget for US-VISIT will need to increased substantially.

Statutory Mandates

One further issue worth mentioning briefly is the confusing legal regime which governs the operations of US-VISIT. Even the exhaustive GAO report has a difficult time cataloging the variety of laws which determine what US-VISIT is required to tackle. The conflicting dictates of the Data Management Improvement Act of 2000, the PATRIOT Act in 2001, the Enhanced Border Security and Visa Entry Reform Act of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004, and annual mandates contained in DHS appropriations laws mean that US-VISIT has been presented with a great deal of flexibility on what to deploy at the land borders of the United States. That flexibility has also made Congress's oversight of US-VISIT difficult and allowed Congress to avoid the tough choices on what it actually expects to be built. This murkiness perhaps gives discretion to the agency best able to make difficult choices on where to spend limited funds, but it also means that there are not measurable deadlines to force decision-making and action.

In sum, within five years, the performance of RFID-equipped credentials and readers should be robust enough to build a land exit system akin to the EZ-P ASS toll lanes now working well around the country. This final phase of US- VISIT will take an additional hundreds of millions of dollars to build the necessary infrastructure and travel documents. If the New York Times can write a similar story about the state of our entry-exit system in 2012, then we will have failed to do what is technologically possible and intellectually wise.

TRANSITION TO TEN-FINGERPRINT CAPABILITY

In July of 2005, a long-running debate between DHS and the Department of Justice concerning how the DHS IDENT fingerprint system and the FBI IAFIS fingerprint system would interact was resolved when Secretary Chertoff announced that US-VISIT and IDENT would migrate to taking ten fingerprints. An interagency user group soon issued a "Challenge to Industry" to build a ten-fingerprint device that could take a full set of fingerprints quickly and accurately. The industry stepped up quickly and has provided the user grouP with machines from several different manufacturers that generally meet the specifications sought by the user group with respect to size, weight, speed, accuracy, ergonomics, and durability. These machines are in testing currently both at DHS and the DOS.

Some 18 months after this "challenge" however, the deployment of the next generation machines has proceeded along a fairly slow track not expected to be completed until the end of 2008. Secretary Chertoff has spoken eloquently about the benefits of the conversion to ten-print

capability including matching travelers against latent prints left at terrorist or crime scenes. The primary delay appears to be based on an inability of the FBI's fingerprint system to handle the volume often-print queries on a real-time basis, as well as the continued construction of the interfaces between the systems, known as the Initial Operating Capability. US-VISIT and the FBI's Criminal Justice Information Service Division have outlined the budget needs to build this capability, but to date less than half of the funds identified have been appropriated to make this interoperability a reality. Hopefully 2007 not only will see rapid procurement of these next generation machines by the DOS and DHS, but also the funding to implement the ten-print vision as the FBI rebrands IAFIS as the Next Generation Identification.

It is worth noting that the deployment of the ten-print machines should not have any negative impacts on travel to the U.S. or wait times at airports. It is expected that travelers will provide all ten prints only once, either at the time of their visa interview or arrival in the U.S. if traveling via the VWP. On subsequent encounters with U.S. frontline officers, taking merely one or two prints on the ten-print device should confirm identity quickly and confidently.

For those who argue that a ten-print system is yet another inconvenience for travelers, it is worth a remainder that scientists at the National Institutes of Science and Technology long have warned that a system of two-print files will eventually grow to a large enough size that the system will begin to genera~ an unacceptable level of false positives. This problem could drastically increase the number of travelers forced to go to secondary processing for ten-print collection and interviews, distracting inspectors from individuals who pose viable threats.

INTERNATIONAL COOPERATION

As the European Union and other countries build their own entry-exit programs, often patterned after the technology and lessons learned from US-VISIT, we need to work aggressively to share information about potential threats, and those who have gone through an intensive background check.

By definition, border management systems involve international cooperation, and the effectiveness of our use of biometrics will depend greatly on our ability to operate effectively in the bilateral and multilateral environments. Negotiating information sharing agreements or playing a leading role in international standards-setting bodies may not be as sexy as deploying new high-tech b~0metric equipment but both are crucial to out success.

Developing information-sharing agreements with foreign partners is a laborious process that has to deal with varying privacy regimes, technical challenges, and concerns about revealing sources and methods of intelligence. However, we know that terrorists and other criminals must use international travel to develop their plots, and the development of robust sharing agreements of biometric and biographic watchlist information should be a high priority. Especially with allies like the United Kingdom and Canada, these types of agreements dramatically increases the odds of using travel checkpoints to find those who need to be detected.

I would make a special mention of the European Union's Visa Information System (VIS) due to come on-line in the next several years. Having negotiated the original treaty on airline passenger data with the EU in 2004, I know how difficult it may be to build interoperability between the

VIS and our Bio Visa/US-VISIT program. Now is the time to begin to tackle that challenge as our citizenries should expect these systems to share valuable intelligence when they are both operational.

In addition, DHS needs to increase dramatically its engagement with foreign governments and international standards setting bodies such as the International Civil Aviation Organization (ICAO). The merger of the BTS Policy office, the DHS Office of International Affairs, and other policy entities in DHS into the new Policy Directorate was a necessary first step. DHS needs to develop a cadre of country specialists and DHS attaches to represent the department in key international locations and to ensure that DHS policymaking does not stop at the water's edge.

Part of this international effort starts at home. Biometrics now playa key role in the security of passports issued to American citizens. Under the electronic passport program developed by the DOS and the Government Printing Office, most new passports now include a biometric facial image and biographic information which is read via a contactless chip by passport readers deployed by DHS. The United States, like many countries around the world developing biometric passports, saw deployment of epassports delayed while technical issues were ironed out in international organizations and privacy concerns were addressed. A well-designed U.S. passport program is essential to securing our own borders to detect foreign imposters and perhaps even those entitled to a U.S. passport with ties to terrorism or serious criminal behavior.

However, there is a major flaw in this program. The United States has never advocated mandatory collection of fingerprint information in foreign passports, in part because it has never required that U.S. citizens provide fingerprints in their own passport applications. This decision needs to be reexamined. In part due to this decision, the United States and the larger world community are building out two elaborate but conflicting border management systems. In the first, governments are going to great lengths to collect terrorist fingerprints along with biographic information, to share such information with other governments, and to ensure that agencies within their government are sharing relevant fingerprints. Within the U.S. government alone, massive efforts have been expended to ensure sharing of relevant biometric information between agencies. In the second system, countries are building elaborate systems of tamper-resistant passports and passport readers capable of doing biometric comparisons; however, neither the mandatory biometric of facial recognition nor one of the optional biometrics, iris scan, can be utilized to find a known terrorist or criminal from a database, because such databases are not available to front-line officers.

The historical resistance of governments to fingerprint law-abiding citizens, not only in the U.S. but in Japan, Australia, and numerous other nations, is weakening. The collective weight of the 70 million non-controversial enrollments in US-VISIT is huge. The program applies to all nationalities and races, has generated no privacy complaints, and has not impacted the speed of border crossings. At a time when terrorists have killed large numbers of people in Asia, Europe, Africa, and other areas of the globe, in addition to North America, people are understandably willing to put aside nervousness about fingerprinting in order to cut off the lifeblood of terrorists - mobility across borders.

Thus I recommend that the U.S. match the bold step of the European Union to include fingerprints in passports and that the U.S. should advocate for fingerprints as a mandatory

biometric in passports at ICAO. At a time when we are going to great lengths to build anti-terrorism and law enforcement systems based on fingerprints, we will never be able to fully engage other countries if we decline ourselves to do what is needed.

Of course governments could attempt to build a regime to allow a one-to-one biometric check between the person who applied for a passport and the person seeking entry based on a facial recognition match. Such a system, however, leaves extensive fingerprint information unutilized and denies us the "bully pulpit" to ask ICAO and other governments to march down the fingerprint path. It is also worth noting that current policy does not allow U.S. passport applicants to be vetted biometrically against criminal or terrorist databases before they are issued passports, meaning we may miss potential imposters or home-grown terrorists or criminals. Nor are we in a strong position to ask other countries to vet their applicants against watchlists they maintain or have rights to access. I am encouraged by the strong efforts of DOS to vet applicants against name-based databases such as the Terrorist Screening Center and certain lists of persons with outstanding warrants, but a fingerprint capability would augment those efforts considerably.

EMPLOYMENT VERIFICATION

As Congress considers comprehensive immigration reform, the US-VISIT biometric platform should be the basis for enrolling and tracking the likely millions of new temporary workers or persons given new legal status in our country. As the recent raids at the Swift meat packing company demonstrate, building any employment verification system solely on Social Security numbers or other forgeable biographic or numeric identifiers is doomed to fail. It appears that an appropriate consensus has developed to allow temporary workers to enter the country or obtain employment only after receiving and presenting a biometric credential at a port of entry and at a workplace.

US-VISIT's proposed end state includes a "person-centric" inventory of all relevant enforcement and immigration services information. When fully-funded and implemented, the program should put an end to the unwieldy and confusing system of records maintained regarding travel and immigration and will result into better service to legitimate travelers and students, and better enforcement tools as well.

Requiring biometric work authorization documents only of foreign workers, however, leaves open the door that they will evade the dictates of their work status by using forged or stolen documents to claim U.S. citizenship or other legal status. While building a universal system of biometric verification at the workplace may have to wait until a subsequent phase of immigration reform, Congress should explicitly preserve the ability of law enforcement agencies to implement such a system. Only when technology and public sentiment converge around this concept will we have an employment enforcement regime that minimizes discrimination, reduces red tape, and provides employers with the certainty they need to hire and train workers. In the meantime, the advent of REAL ID and driver's licenses that can be authenticated via embedded watermark technology should provide employers with an ability to detect bogus documents with greater ease at a reasonable cost.

CONCLUSION

US-VISIT was and remains an extremely difficult program to' execute. But for 2007, let's focus on the six challenges above, and build on the truly historic achievement USVISIT represents: restoring control and integrity to our borders after decades of neglect without destroying the attractiveness of the United States as a place to study, conduct research or business, or see friends or family.

1 Monument Policy Group represents several clients with a variety of interests related to immigration
matters and CSIS does not take policy positions; thus, this testimony is submitted in my personal capacity
arid not on behalf of any third party.