June 2005

REPORT

REAL CHALLENGES FOR VIRTUAL BORDERS:

The Implementation of US-VISIT

Rey Koslowski
Associate Professor of Political Science
Rutgers University–Newark

mpi
MIGRATION POLICY INSTITUTE

REAL CHALLENGES FOR VIRTUAL BORDERS:

The Implementation of US-VISIT

Rey Koslowski
Associate Professor of Political Science
Rutgers University–Newark

mpi
MIGRATION POLICY INSTITUTE

TABLE OF CONTENTS

I. INTRODUCTION

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program is developing an automated entry-exit tracking system that collects biographical and biometric data from foreign nationals at US consulates abroad as well as when they enter the United States. Watch list checks are run on the data collected in order to help inspectors at ports-of-entry keep out potential terrorists and criminals as well as determine whether those who enter the United States leave in accordance with the terms of their visas. The entry-exit tracking system at the core of US-VISIT was initially envisioned to enforce immigration law, but was then recast into a counterterrorism role after September 11, 2001.

US-VISIT is an integral part of the Bush administration's efforts to create a "smart border," which "must integrate actions abroad to screen goods and people prior to their arrival in sovereign US territory, …allow extensive prescreening of low-risk traffic, thereby allowing limited assets to focus attention on high-risk traffic, [and] use… advanced technology to track the movement of cargo and the entry and exit of individuals."[1] In a dramatic illustration of the administration's agenda, Richard Falkenrath, former deputy assistant to the president and deputy Homeland Security advisor, drew an analogy likening the revolution in military affairs of the 1990s to the "revolution in border security" that is taking place now.[2]

The US National Homeland Security Strategy advocates "pushing borders out" beyond US territorial boundaries by stationing Customs and Border Protection (CBP) officers in seaports and airports abroad and by requiring electronic submission of passenger and cargo manifests in

1 "Fact Sheet: Border Security," The White House, January 25, 2002, http://www.whitehouse.gov/news/releases/2002/01/20020125.html (accessed January 27, 2005).

2 Response to author's question at "Transatlantic Homeland Security? European Approaches to 'Total Defense,' 'Societal Security' and Their Implications for the US," Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University, February 19, 2004.

advance of departure to the United States. As expanding e-government and private sector submission of electronic data enables the preclearance of passengers and cargo, thereby removing the necessity of inspection at territorial boundaries, borders may increasingly exist de facto in cyberspace, i.e., become "virtual borders."

The Department of Homeland Security contracted with a team of companies in May 2004 to realize its vision for US-VISIT "to deploy end-to-end management of processes and data on foreign nationals to the United States covering their interactions with US officials before they enter, when they enter, while they are in the United States, and when they exit. This comprehensive view of border management will lead to the creation of a 'virtual border.'"[3] Congress mandated the deployment of an automated entry-exit system at all ports-of-entry by the end of 2005. However, this more comprehensive vision for US-VISIT is expected to be developed and deployed over the coming five to ten years.

This report will evaluate US-VISIT within the broader contexts of national and homeland security as well as immigration law enforcement and policymaking. This evaluation is primarily based on the review of government documents as well as discussions with policymakers and stakeholders in Washington, DC, San Diego/Tijuana, and Detroit-Windsor; participation in not-for-attribution roundtable discussions with policymakers; public meetings; and congressional hearings. The intent of the report is constructive criticism, which may be useful in rethinking approaches and formulating midcourse corrections given that the system will not be fully developed and deployed until the end of this decade at the earliest. Since the publicly available information on US-VISIT does not fully specify the shape of the future system and the range of people who will ultimately be subject to it, this report also includes some speculation.

Even when fully deployed, US-VISIT can only be a small part of the counterterrorism toolkit. US-VISIT is becoming an additional obstacle

3 "Request for Proposals for US-VISIT Program Prime Contractor Acquisition," RFP no. HSSCHQ-04-R-0096, US-VISIT Office, Department of Homeland Security, November 28, 2003.

to foreign terrorists wishing to enter the country, but it is unlikely itself to catch many terrorists trying to enter the United States. "Established" terrorists with track records within the intelligence community are unlikely to voluntarily submit their biographical and biometric data at US consulates and ports-of-entry. "Potential" future terrorists are unlikely to have generated intelligence records that would trigger a watch list hit in the system. Although US-VISIT is unlikely to catch many terrorists, it may deter some terrorists and deflect those who are more determined toward more difficult crossings.

There are many technical, physical, political, and economic challenges to the implementation of US-VISIT, even if only to enforce immigration laws. No matter how "smart" borders become, they cannot become totally virtual. Most notably, significant investments in physical infrastructure at the border will be necessary to enable new technologies to work their magic. More trained inspection personnel will still be required to ensure adequate inspection of travel documents. Information systems also require accurate and complete data to be effective, and there are major gaps in the data being entered into the individual systems that currently make up US-VISIT as well as limitations on the interoperability of that data.

It is, therefore, not clear that US-VISIT's potential benefits justify the necessary investments in border infrastructure, data acquisition, human resources, and other resources to make it work as envisioned or that the president and Congress are willing to expend sufficient "political capital" to overcome these barriers. If the political will is lacking to undertake some potentially very expensive and unpopular measures necessary for effective deployment of US-VISIT, it may be better to scale back the requirements—and expectations—of the program rather than develop a problem-ridden, partially deployed system that cannot accomplish the unrealistic goals set out for it.

II. BORDER CONTROL AFTER SEPTEMBER 11, 2001

The September 11 attacks exposed the security consequences of increasing migration and travel, as terrorists used visa and identity document fraud to enter the United States. Al Qaeda operated a "passport office" at the Kandahar airport to alter travel documents and train operatives, including Mohamad Atta.[4] At least two, and perhaps as many as eleven, of the September 11 hijackers used fraudulently altered passports. One of the hijackers entered with a student visa but never showed up for class; three had stayed in the United States after their visas expired; and several purchased fraudulent identity documents on the black market that primarily services illegal migrants.[5] Contrary to many of the early discussions in the media that claimed all of the hijackers entered legally and that border controls were therefore irrelevant to their entry, the 9-11 Commission concluded that "15 of the 19 hijackers were potentially vulnerable to interception by border authorities."[6] The 9-11 Commission staff report on terrorist travel also details linkages between human smugglers and Al-Qaeda and other terrorist groups in need of travel facilitation.[7]

---

4 The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (New York: W.W. Norton 2004), 169.

5 "Ziad Jarrah attended flight school in June 2000 without properly adjusting his immigration status, thereby violating his immigration status and rendering him inadmissible under 8 USC. § 1182(a)(7)(B) each of the subsequent six times he reentered the United States between June 2000 and August 5, 2001. (Hani) Hanjour did not attend school after entering on a student visa in December 2000, thereby violating his immigration status and making him deportable under 8 USC. § 1227(a)(1)(B). Mohamed Atta failed to present a proper M-1 (vocational school) visa when he entered the United States in January 2001. He had previously overstayed his tourist visa and therefore was inadmissible under 8 USC. § 1182(a)(7)(B). Nawaf al Hazmi and Suqami overstayed the terms of their admission, a violation of immigration laws rendering them both deportable under 8 USC. § 1227(a)(1)(B)," (9/11 Commission 2004a: 138-39).

6 Ibid., 384.

7 *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*, (9/11 Commission 2004a).

The Department of Homeland Security (DHS) was established to increase transportation and border security, minimize the risk of another terrorist attack, and prepare to respond to any future attacks that may occur. The DHS's Bureau of Customs and Border Protection (CBP) has the task of intercepting terrorists, enforcing immigration law, and collecting customs duties at 326 air, sea, and land ports-of-entry and preclearance stations,[8] and between ports-of-entry along the 5,525-mile US–Canadian border and the 1,989-mile US–Mexican border. At the same time, CBP is charged with facilitating lawful trade and travel at those ports-of-entry. Approximately 433 million people were inspected upon entry into the United States in fiscal year (FY) 2004. Of those, 337 million crossed the land border, 77 million entered through airports, 14 million entered seaports, and 628,290 were denied entry.[9] It has been estimated that there are now about ten million undocumented migrants in the United States, approximately 30 to 40 percent of whom entered legally but overstayed their visas.

The attacks of September 11, 2001, demonstrated the vulnerability of the US economy to shutdowns of the transportation system. The grounding of commercial air traffic and heightened border security after the September 11 attacks amounted to the United States doing to itself what no enemy had done before: an embargo on trade.[10] This self-embargo demonstrated the vulnerability of extended supply chains and transborder, just-in-time manufacturing, most dramatically on the US–Canadian border. Up to ten million vehicles annually cross the Ambassador Bridge between Windsor, Ontario, and Detroit, Michigan, along with approximately 25 percent of US–Canadian merchandise trade. Shortly after the attacks, traffic backed up by as much as fifteen hours. Within days, Daimler-Chrysler announced that it would have to stop several US assembly lines for want of Canadian parts caught in traffic backups at the border. More than any other event, these

8 "There are 312 official ports-of-entry in the United States and fourteen preclearance stations in Canada and the Caribbean, a total of 326 officially manned and unmanned ports," http://www.cbp.gov/xp/cgov/toolbox/ports/.

9 See Immigration Monthly Statistical Report, September 2004 Year End Report at http://uscis.gov/graphics/shared/aboutus/statistics/msrsep04/INSP.HTM.

10 Stephen E. Flynn, "America the Vulnerable," *Foreign Affairs* 81, no. 1 (Jan./Feb. 2002): 60-74.

backups at the US–Canadian border precipitated the US–Canadian "Smart Borders" Declaration[11] and prompted the Bush administration to adopt the information technology–enabled, risk management approach to border control that resulted in increased budgets for border control information technologies.

III. US-VISIT AND HOW IT WORKS

A. The development of US-VISIT

Although many policy initiatives and the associated border control information technology that underlies the smart borders approach existed before September 11, 2001, it was the attacks on that day that led Congress to demand their implementation. Section 110 of the US Illegal Immigration Reform and Immigrant Responsibility Act of 1996 had mandated that the Immigration and Naturalization Service (INS) develop an automated entry-exit control system that would "collect a record of every alien departing the United States and match the records of departure with the record of the alien's arrival in the United States."[12] This was to be done by the end of 1998. The original purpose of the system was not related to preventing criminal entry or counterterrorism, but to addressing the issue of visa overstays.

Congress pushed back the deadline for implementation of the law in October 1998 after lobbying by US business groups, states, and localities bordering Canada and Mexico.[13] These groups pointed out that

11 For an evaluation of the Smart Border agreements with Canada and Mexico, see Deborah Waller Meyers, "Does 'Smarter' Lead to Safer? An Assessment of the Border Accords With Canada and Mexico," *MPI Insight*, (Migration Policy Institute), no. 2 (June 2003).

12 *Illegal Immigration Reform and Immigrant Responsibility Act of 1996*, section 110.a.1, "Automated Entry-Exit Control System," US Congressional Record—House (September 28, 1996): H11787.

13 Theodore H. Cohn, "Cross-Border Travel in North America: The Challenge of US Section 110 Legislation," *Canadian American Public Policy*, (Occasional Paper Series of the Canadian-American Center, University of Maine at Orono), no. 40 (October 1999): 25-38.

registering every person who crosses into the United States from Canada or Mexico, even using then-existing smart card technology, would still require enough processing time to back up traffic at the border for hours, especially at the Detroit-Windsor crossing.[14] The Data Management Improvement Act (DMIA) of 2000 amended Section 110, mandating the development of an entry-exit system to be put in place at all air and seaports by the end of 2003, at the fifty most highly trafficked land ports-of-entry by the end of 2004, and at all ports-of-entry by the end of 2005. In practical terms, however, the DMIA deflected the creation of a full-fledged entry-exit system with a complete database since it limited data collection to that which was already being collected by the INS by existing authorities of law and disallowed collection of any new entry-exit data.[15]

The entry-exit tracking system that existed prior to September 11, 2001, primarily covered passengers arriving by airplane and consisted of a paper I-94 form stamped at the port-of-entry, which was supposed to be collected by the airline upon departure, given to the INS, then sent by the INS to a contractor who manually entered the data into the database of the legacy INS Nonimmigrant Information System (NIIS). Due to lost forms, incomplete or inaccurate data entry, exit by land border, and incomplete deployment of the system, missing exit data corrupted the database, leaving inspectors with no effective way of knowing if individuals had overstayed their visas.[16] This was the case with several of the September 11 hijackers.

For example, an INS inspector at Miami International Airport stopped Mohamed Atta on January 10, 2001, when Atta said that he was planning to take flight lessons but was entering the country on a tourist visa rather than a vocational education visa. He was detained for additional questioning by another officer, and after almost an hour he was released. Neither officer noticed that he had overstayed his visa by more than a month on his previous trip to the United States. A former

14 Senate Judiciary Committee Report, submitted with *The Border Improvement and Immigration Act of 1998*, Senate Report 105-197.

15 See *Data Management Improvement Act of 2000*, Public Law 106-215.

16 Statement of Michael R. Bromwich before the House Judiciary Committee, Subcommittee on Immigration and Claims, March 18, 1999.

INS inspector, Patrick Pizarro, explained that the inspectors most likely missed Atta's overstay because they were under pressure to clear tourists as quickly as possible, yet "You don't have all the information about every arriving passenger in one database," Pizzaro said. "It's all scattered in various databases and it's time-consuming to find the information you need."[17] After September 11, incoming passengers received greater scrutiny, but according to an INS inspector from Miami who appeared on CBS's *60 Minutes* against his supervisor's wishes, the systems were down once or twice a week, and passengers were still being admitted without having been checked against the lookout databases.[18]

In response to the September 11 attacks and the failures of government information systems that they exposed, Congress passed and President Bush signed into law entry-exit system provisions in the USA PATRIOT Act[19] and in the Enhanced Border Security and Visa Entry Reform Act of 2002.[20] Both pieces of legislation reiterated the DMIA mandate for implementation of an entry-exit system. The USA PATRIOT Act mandated that the entry-exit system should utilize biometric technology and tamper-resistant, machine-readable documents, and that the system should be able to interface with other law enforcement databases. The Enhanced Border Security and Visa Entry Reform Act, passed in the Senate by a margin of 97 to 0 and in the House 411 to 0, specifically required the development of a database for arrival and departure data from machine-readable travel documents, the establishment of standards for biometrics for visas and other travel documents, and the installation of equipment at all ports-of-entry to enable collection, comparison, and authentication of biometric data. In order to address the loopholes that allowed some members of Al Qaeda to enter on US visas, Congress mandated that all US visas incorporate a biometric

17 Quoted in Alfonso Chardy, "Atta faced questions about visa at MIA, Flying-lesson plans aroused suspicion," *The Miami Herald*, October 19, 2001.

18 "INS Vigilance Under Fire," *60 Minutes*, CBS News, March 10, 2002.

19 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Public Law 107-56, section 414 (October 26, 2001).

20 *Enhanced Border Security and Visa Entry Reform Act of 2002*, Public Law 107–173, section 302 (May 14, 2002).

identifier by October 26, 2004, and a combination of facial recognition and electronic fingerprint scanning was selected as "the most effective and least intrusive."[21]

Most recently, the Intelligence Reform and Terrorism Prevention Act of 2004 called for an acceleration of the full implementation of an automated biometric entry-exit data system; collection of biometric exit data from all those required to provide biometrics upon entry; integration of all databases that contain information on aliens and interoperability with the entry-exit system; policies and procedures to maintain accuracy and integrity of entry-exit data; frontline personnel training; and a registered traveler program that is integrated into the automated, biometric entry-exit system.[22]

After the September 11 attacks, border management agencies created an Integrated Program Team (IPT), originally known as the Entry-Exit Program Team. This team developed the Visa Waiver Permanent Program Act Support System (VWPASS) and the National Security Entry-Exit Registration System (NSEERS). On April 29, 2003, the newly established Department of Homeland Security announced the consolidation and revamping of these programs to form the new US-VISIT program. The US-VISIT program is housed within the Border and Transportation Security (BTS) Directorate. The program team includes representatives from CBP, Immigration and Customs Enforcement (ICE), and the Transportation Security Agency (TSA). The program spans the DHS, with representatives from US Citizenship and Immigration Services (USCIS), the Directorate for Management, and the Science and Technology Division. The program also reaches outside DHS, with representatives from the departments of Transportation, State, Commerce, and Justice and from the General Services Administration (GSA).

On July 8, 2003, the US-VISIT program sponsored an Industry Day at which program staff presented their system requirements to

21 "Post 9/11 Visa Reforms and New Technology: Achieving the Necessary Improvements in a Global Environment," testimony of Janice L. Jacobs, deputy assistant secretary for consular affairs, before the Senate Foreign Relations Committee, October 23, 2003.

22 *The Intelligence Reform and Terrorism Prevention Act of 2004*, House Report 108-796, Section 7208.

prospective contract bidders and asked the firms for their input. As US-VISIT director Jim Williams put it, "I really envision this as a partnership every step of the way, a seat at the table….We want the prime integrator to play a key role with every aspect."[23]

In the subsequent request for proposals (RFP), the US-VISIT program set out the mission of US-VISIT to "collect, maintain, and share information on foreign nationals, including biometric identifiers, through a dynamic, interoperable system that determines whether the individual: should be prohibited from entering the US; can receive, extend, change, or adjust immigration status; has overstayed or otherwise violated the terms of their admission; should be apprehended or detained for law enforcement action; needs special protection/attention (i.e., refugees)."[24]

A prime contractor and its team of companies were to develop the comprehensive system envisioned to achieve that mission, and at the end of May 2004, a team led by Accenture was selected. The US-VISIT program's cumulative budget added up to well over $1 billion through the end of FY2005.[25] In addition, President Bush has proposed $390 million for US-VISIT in FY2006.[26] Looking towards the future, the DHS has estimated that the overall cost of the system would be $7.2 billion through FY2014, but the Government Accountability Office (GAO) calculated that its ten-year cost could be as much as twice that.[27]

B. Implementation increments, systems, and processes

In accordance with congressional mandates, US-VISIT is being implemented incrementally.[28] Increment 1 of US-VISIT went live January 5,

23 Quoted in Sara Michael, "US-VISIT Requirements Outlined," *Federal Computer Week*, July 8, 2003.

24 "Request for Proposals for US-VISIT Program Prime Contractor Acquisition," RFP no. HSSCHQ-04-R-0096, US-VISIT Office, Department of Homeland Security, November 28, 2003.

25 "Budget in Brief, Fiscal Year 2005," Department of Homeland Security.

26 "Budget in Brief, Fiscal Year 2006," Department of Homeland Security.

27 Randolf C. Hite, testimony for oversight hearing, "US-VISIT—A Down Payment on Homeland Security," House Committee on the Judiciary, March 18, 2004.

28 See "Request for Proposals for US-VISIT Program Prime Contractor Acquisition," op. cit., and "Some Progress Made, but Many Challenges Remain on US Visitor and Immigrant Status Indicator Technology Program," Government Accountability Office, GAO-05-202, February 2005.

2004, when the DHS began to collect digital photographs and fingerprint scan biometrics from those individuals traveling on a nonimmigrant visa to the United States upon entry at 115 airports and fourteen seaports. Exit capability was initially limited to two pilot projects at Baltimore-Washington International Airport (BWI) and Miami Seaport. In August and November of 2004, pilot projects were extended to twelve additional airports and one seaport. Increment 2A was to deploy equipment and software at all ports-of-entry, to capture biometric data from machine-readable travel documents by October 26, 2004, but this deadline was extended. Increment 2B involved deploying the entry capabilities of Increment 1 at the fifty highest-volume land ports-of-entry by December 31, 2004. Increment 2C involves pilot deployment of a radio frequency (RF) system that captures biographical data at exit as well as entry at one or more land ports-of-entry by June 30, 2005. Increment 3 extends Increment 2B capability to the remaining 115 land ports-of-entry by December 31, 2005. Increment 4 will be an expanded set of releases of the envisioned, integrated solution to be developed by the Accenture-led team.

The preentry process, as it currently exists, begins at US consulates abroad. Nonimmigrant visa applicants provide biographic data on the visa application and submit a digital photograph and fingerprint scans at US embassies and consulates. These data are checked against the Consular Lookout and Support System (CLASS) watch list, which includes data from the Justice Department's National Crime Information Center (NCIC) system, a computerized index of criminal justice information (criminal records, fugitives, terrorist lookouts, missing persons, etc.) as well as other Interagency Border Inspection System (IBIS) watch lists. A record is then generated within IBIS. IBIS is a system shared by twenty law enforcement and border control agencies that resides on the Treasury Enforcement Communication System (TECS) at the CBP Data Center. After watch list checks are run, the visa application is either approved or denied. When those who have received a visa board a US-bound airplane or ship, the airlines and sea carriers are required to electronically transmit passenger manifests using the Advance Passenger Information System (APIS). Passenger data on these manifests are then checked against watch lists in advance of arrival at US ports-of-entry.

US-VISIT Component Systems

According to the US-VISIT RFP,[29] the requirements of the first three increments are being met by extending, enhancing, and building interfaces between some (and potentially all) of the following legacy systems:[30]

Arrival Departure Information System/Visa Waiver Permanent Program Act Support System (ADIS/VWPASS)
Advance Passenger Information System (APIS)
Biometric Verification System (BVS)
Consolidated Consular Database (CCD)
Central Index System (CIS)
Computer-Linked Application Information Management System (CLAIMS)
Consular Lookout and Support System (CLASS)
Global Enrollment System (GES)
Integrated Automated Fingerprint Information System (IAFIS)
Interagency Border Inspection System (IBIS)
INS Automated Biometric Identification System (IDENT)
Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS)
National Automated Immigration Lookout System (NAILS II)
NEXUS
Nonimmigrant Information System (NIIS)
Outlying Area Reporting Station (OARS)
Portable Automated Lookout System (PALS)
Secure Electronic Network for Travelers Rapid Inspection (SENTRI)
Student Exchange and Visitor Information System (SEVIS)

Since the preparation of the RFP, some of these systems may have been decommissioned or merged into other systems. Some of these systems may remain in existence independent of US-VISIT, even though they interface with US-VISIT. Other systems may eventually disappear as stand-alone systems as all of their functions are incorporated into another component of US-VISIT. From all public indications, however, it appears that for the foreseeable future the US-VISIT system will be made up of these interfaced systems, and the system envisioned in Increment 4 will build on, add to, and extend the capabilities of these systems. There is a debate within the DHS as to whether at some point a completely new system should be built to which all US-VISIT functions would migrate, thus terminating all legacy systems.

The entry process, as it currently exists at air and seaports, begins when a foreign national arrives at the primary inspection site and presents his or her travel documents to the inspector. The inspector scans the machine-readable documents (or enters data manually if documents are not machine-readable) into IBIS. The Inspector Field Manual requires that in primary inspections, inspectors must run queries of IBIS using the foreign national's last name, first name, date of birth, and passport number.[31] IBIS and APIS queries generate any existing biographical lookout hits and existing records based on manifest data. IBIS also indicates if there are any existing fingerprints in the IDENT database that were submitted during the visa application process. Once a biographical record is generated from the Consolidated Consular Database (CCD) or from passenger manifest data, the inspector switches to the IDENT screen, takes the person's photograph, and scans each index finger. These biometrics are checked against the IDENT database. If there are no fingerprints in the database, the person is enrolled in US-VISIT; if there are fingerprints that were submitted during the visa application process, a one-to-one match with data from the initial enrollment abroad verifies the individual's identity.[32] If there is a watch list hit or a biometric mismatch, the person goes to secondary inspection for additional screening.[33]

In the exit process, as it currently exists, air and sea carriers transmit electronic manifest data though APIS, which is then matched to entry records in ADIS for a corresponding entry-exit confirmation. At the thirteen airports and two seaports where the exit process is being piloted, departing visitors "check out" of the country at self-serve US-VISIT exit stations or with attendants at the departure gate in one

29 See "Request for Proposals for US-VISIT Program Prime Contractor Acquisition," op. cit. 3

30 Other systems may feed data to US-VISIT or may be interfaced in the future but were not on this list in the RFP.

31 "A Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States," Department of Homeland Security, Office of Inspector General, OIG-05-07 December 2004, 15.

32 As it stands, digital photographs and fingerprints from previous enrollments are not available to the officer conducting the primary inspection.

33 "First Phase of Visitor and Immigration Status Program Operating, but Improvements Needed," General Accounting Office, GAO-04-586, May 2004.

of three ways: 1) at self-service exit stations, visitors place their two index fingers on the scanner, have a digital photograph taken, and receive a printed receipt that verifies checkout; attendants are available for assistance; 2) an additional step is added in which a US-VISIT attendant at the departure gate verifies departure by scanning the receipt from the exit station and taking another finger scan with a portable reader to match to the receipt; 3) visitors are checked out at the departure gate by a US-VISIT attendant using a portable biometric reader/exit processing device. In the initial two pilots, biometric data collected from exit stations are burned onto a CD-ROM at the end of each day and mailed by express service to a contracting firm that enters the data into IDENT, which executes a one-to-one match comparing the exit to the entry record.[34]

C. Related programs and systems

As the envisioned US-VISIT system develops, it will more fully incorporate the functions of the National Security Entry-Exit Registration System (NSEERS), Student Exchange Visitor Information System (SEVIS), and registered traveler systems such as INSPASS, NEXUS, and SENTRI. Indeed, the DHS is now proposing to establish the Office of Screening Coordination and Operations (SCO) within the Border and Transportation Security (BTS) Directorate in order to consolidate various screening efforts and enhance terrorist-related screening "through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, and other entities and objects that pose a threat to homeland security."[35] This new office would encompass US-VISIT; NEXUS; SENTRI; Secure Flight and Crew Vetting; Free and Secure Trade (FAST); Transportation Worker Identification Credential (TWIC); Registered Traveler; Hazardous Materials Trucker Background Checks; and Alien Flight School Checks. The proposed FY2006 budget for the SCO is approximately $847 million, of which $390 million is dedicated to US-VISIT.[36]

34 Ibid.

35 "Budget in Brief, Fiscal Year 2006," op. cit, 6.

36 Ibid., 15.

The NSEERS program was initiated on September 11, 2002, and it has been described by Immigration and Customs Enforcement (ICE) as "the first step taken by the Department of Justice and then DHS in order to comply with the development of the Congressionally-mandated requirement for a comprehensive entry-exit program by 2005."[37] "Special registration," as the process is also known, created a national registry for nonimmigrant aliens initially from countries that were deemed high risk from a security standpoint. Nationals of Iran, Iraq, Libya, Syria, and Sudan are required to register at ports-of-entry, and based on initial questioning upon arrival, CBP officers could require registration of foreign nationals from all other countries, if deemed necessary.[38] NSEERS collects photographs and fingerprints from these visiting foreigners as well as detailed information about the background and purpose of their visit to the United States. Those who are entered into NSEERS at entry must also register their departure at one of the specially designated ports and appear before a CBP officer.

Until cancellation in December 2003, there had also been an additional requirement for a thirty to forty-day follow-up interview for those who were registered at a port-of-entry as well as an annual registration requirement. Known as "domestic registration," this requirement was imposed on males over sixteen years of age from Afghanistan, Algeria, Bahrain, Bangladesh, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kuwait, Libya, Lebanon, Morocco, North Korea, Oman, Pakistan, Qatar, Somalia, Saudi Arabia, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen. As of September 30, 2003, nationals of 150 countries have been registered in NSEERS for a total of 290,526 registrations: 207,007 registrations (93,741 individuals) at ports-of-entry and 83,519 individuals at the former INS offices.[39] When US-VISIT is fully deployed, with complete entry and exit capabilities at all ports and with an integrated status management system, it is expected that the separate biometric entry-exit enrollment features of the NSEERS

37 "Changes to National Security Entry/Exit Registration System (NSEERS)," Fact Sheet, Immigration and Customs Enforcement, December 1, 2003, http://www.ice.gov/graphics/news/factsheets/nseersFS120103.htm (accessed January 25, 2005).

38 For example, those born in Iran, Iraq, Libya, and Syria who were naturalized elsewhere.

39 "Changes to National Security Entry/Exit Registration System (NSEERS)," op. cit.

program can be eliminated. However, the more detailed interviews and background checks of special interest persons of the NSEERS program will most likely continue.

SEVIS is a system designed to maintain data on foreign students and exchange visitors and their dependents. The system is administered by Immigration and Customs Enforcement (ICE) and used by CBP to register entries and exits. Mandated by 1996 legislation, SEVIS had been deployed on a pilot basis before September 11, 2001, after which Congress mandated full-scale deployment so that schools could use the Web-based system by January 30, 2003, and so that all students and exchange visitors could be registered with SEVIS by August 1, 2003. One year later, 8,737 schools were using the system, and the data of more than 770,000 students and exchange visitors, as well as 100,000 dependents, were being managed by the system.[40] Together with the Computer-Linked Application Information Management System (CLAIMS 3), SEVIS is central to the existing US-VISIT status management capability. As the system envisioned for Increment 4 of US-VISIT develops an increasingly robust status management capability, it may or may not be necessary for SEVIS to continue as an additional, standalone system, depending on how other SEVIS functions such as the registration of schools authorized to enroll foreign students, work authorization, and reinstatement of status are handled.

The Passenger Accelerated Service System (INSPASS) is a legacy INS program started in the mid-1990s that uses a database linked to a hand geometry recognition system. US citizens and noncitizens (nationals of Canada, Bermuda, and Visa Waiver Countries) who are frequent fliers, are traveling on certain visas, and are willing to give personal and passport data for a background check, as well as a digitized biometric reading of their hand for entry into the database, could be expedited through passport controls. According to a fact sheet posted on the "Frequent Traveler Programs" page of the CBP Web site,[41] INSPASS is at six international airports: Los Angeles, CA (LAX);

40 "SEVIS—Year Two," Department of Homeland Security, Fact Sheet, August 27, 2004.

41 See "INS Passenger Accelerated Service System (INSPASS)" (last modified 06/21/2004), http://www.cbp.gov/xp/cgov/travel/frequent_traveler/ (accessed January 25, 2005).

Newark, NJ (EWR); John F. Kennedy, NY (JFK); Washington Dulles, VA (IAD); and the US preclearance sites at Vancouver and Toronto in Canada. INSPASS lanes are suspended, however, when the terrorist threat level goes to orange. However, based on personal observation at several of these airports, INSPASS no longer appears to be operative. INSPASS may in some respects be a model for the Transportation Security Agency (TSA)'s Registered Traveler pilot program, which is available to US nationals and legal permanent residents for expedited treatment at some TSA airport security screening locations.

NEXUS and SENTRI are preapproved passenger vehicle programs in which registered travelers enroll by submitting information for criminal and terrorist background checks. NEXUS is jointly administered by the United States and Canada; the SENTRI program operates at ports-of-entry along the US border with Mexico. After a NEXUS enrollee clears the background check, he or she receives a radio frequency (RF)-enabled proximity card. The RF-enabled chip on this card is read at the port-of-entry and automatically pulls up background information and a photo for an inspector. The inspector can then quickly verify the NEXUS cardholder's identity and wave him or her through. The SENTRI process is similar except that it is vehicle-based and a radio frequency identification (RFID) transponder is attached to the enrollee's car. There are plans to transform SENTRI into a person-based system with individual proximity cards. Although interfaces had not been built to connect NEXUS and SENTRI to US-VISIT,[42] the Intelligence Reform and Terrorism Prevention Act of 2004 requires that such registered traveler programs be integrated into the biometric entry and exit data system.

Initially, the requirement for biometric enrollment in US-VISIT upon entry into the United States did not apply to nationals of the twenty-seven states in the US Visa Waiver Program (VWP) who are permitted to enter and stay in the United States without a visa for up to ninety days. The original idea was that these countries would include biographic and digitized biometric data in machine-readable passports in order for border control authorities to securely establish their

42 Author's discussion with DHS official, April 9, 2004.

nationals' identities and facilitate biographic and biometric watch list checks. The Enhanced Border Security and Visa Entry Reform Act conditioned countries' participation on the issuance of machine-readable, tamper-resistant passports containing biometric data and set a deadline of October 26, 2004. After many countries informed the State Department and the DHS that they could not meet this deadline, former secretaries Tom Ridge and Colin Powell asked Congress for a postponement to December 2006,[43] and Congress granted a one-year extension to October 26, 2005.[44] In conjunction with the deadline extension request, the DHS announced that nationals of the twenty-seven Visa Waiver countries would be required to enroll in US-VISIT and submit to a digital photograph and finger scanning upon entry beginning September 30, 2004.

The US Congress deferred to the International Civil Aviation Organization (ICAO) on setting the biometric standards for passports issued by Visa Waiver countries, and it was not until May 28, 2003, that ICAO announced an agreement—a digital photo for facial recognition plus optional biometrics of fingers and/or eyes, which are stored on contactless integrated circuit (IC) chips.[45] The contactless IC chip is part of a radio frequency (RF) system in which data on the IC chip is transmitted via radio waves to a reader. The reader provides the power; the contactless IC chips are passive and do not require batteries. In contrast with machine-readable travel documents that contain data on magnetic strips, a passport with a contactless chip can be scanned by the reader at a distance, therefore allowing faster transfer of data from the passport.

As originally envisioned, holders of new biometric passports issued by Visa Waiver countries will give their passports to CBP inspectors who

43 Colin Powell and Tom Ridge, letter to Jim Sensenbrenner Jr., chairman, Committee on the Judiciary, House of Representatives, March 17, 2004, http://www.house.gov/judiciary/ridge031704.pdf (accessed March 29, 2004).

44 See "An Act: To modify certain deadlines pertaining to machine-readable, tamper-resistant entry and exit documents," H.R. 4417.

45 "Biometric Identification to Provide Enhanced Security and Speedier Border Clearance for the Travelling Public," International Civil Aviation Organization, PIO/2003 (28 May 2003), http://www.icao.int/icao/en/nr/2003/pio200309.htm (accessed November 20, 2003).

will simply bring the passport close to the reader. The reader will capture the personal data and the digitized biometrics. This information can then be checked against terrorist and law enforcement watch lists. If there are no hits, the inspector can then allow the traveler to continue on through passport control and enter the United States. Similarly, upon exiting within the ninety-day limit of the Visa Waiver Program, the traveler will "check out" of the country with a wave of the passport over a reader, possibly even using a self-service kiosk. With the US-VISIT enrollment requirement now in place for nationals of Visa Waiver Program countries, it is not clear that biometric passports will ever be able to serve in this way, because it is unclear that the US-VISIT enrollment requirement will ever be rescinded in the future.

IV. CHALLENGES

A. Multiple missions

The entry-exit system at the heart of US-VISIT was originally designed to determine whether visiting foreigners overstayed their visas, but was recast after the September 11 attacks as a system to combat terrorism. According to DHS, US-VISIT now has both immigration law enforcement and antiterrorism missions. There are serious limitations, however, as to what US-VISIT can accomplish with respect to each of these missions, and the requirements for each may conflict. US-VISIT will provide much better visa overstay data, but this data might not be that useful for the apprehension and prosecution of visa overstayers. On the counterterrorism front, it is likely that US-VISIT will only be able to deter or divert terrorists, not catch them. These inherent limitations call into question the ambitiousness of the goals set out for the system and raise the issues of goal prioritization, implementation reconsiderations, and deadline expectations.

With respect to the immigration law enforcement mission, an automated entry-exit system may be the only effective way to identify individual

visa overstayers, gather aggregate data to confirm the estimates of some 2.3 million visa overstayers who filled out I-94 forms, determine the additional Mexican and Canadian overstayers, and calculate more accurate overstay rates of nationals of states applying for the Visa Waiver Program so as to make better assessments of program eligibility.[46]

The utility of an entry-exit system in apprehending and prosecuting individual visa overstayers, however, is not so clear cut. The database would have to be accurate enough to ensure that the lack of an exit record truly meant that the person in question actually had not left the country. If there were to be repeated errors in the exit data that could be corroborated by other evidence (e.g., the name of the person on an outbound airline manifest, an entry stamp in the individual's passport from another country before the individual's US visa expired, combined with boarding passes, home videos documenting the individual's homecoming, etc.), then the entry-exit system could be considered unreliable as a whole and the data it generated not useful for the prosecution of individual cases. If one individual could register an exit of another without being detected by the entry-exit system, it could be susceptible to fraud. Once identified, it is unlikely that a visa overstayer would remain at the address originally given upon arrival, and even if he or she did, there are a limited number of ICE officers available to find, apprehend, and deport millions of visa overstayers.[47]

Although it is clear that an automated entry-exit system cannot also automatically enforce visa time limitations, such a system constrains the options open to visa overstayers that may, in turn, modify their behavior. Most importantly, individuals may be able to overstay their visas once (meaning avoiding discovery and remaining in the United States), but it would be very difficult for them to leave the United States, apply for another visa, and overstay again. For example, a Polish roofer with US relatives may apply for a thirty-day tourist visa with the purpose of visiting family at Easter, then stay and work through the building season and return home at the end of fall. Having

46 "Overstay Tracking: A Key Component of Homeland Security and a Layered Defense," General Accounting Office, GAO-04-82, May 2004.

47 Senate Report 105-197, op. cit., 14-16.

earned a significant amount of money in the United States, he may deposit a relatively substantial amount in the savings account of a Polish bank and purchase some property in Poland. The savings and property demonstrate financial solvency and provide a reason for his return to Poland, thereby setting the stage for another successful tourist visa application two years later, again to visit family and again to work though the building season.

Without a credible entry-exit system, it has been possible for visa overstayers to not only stay in the United States, but also to travel back and forth. If nothing else, US-VISIT could reduce the total number of visa overstayers in the United States simply by stopping those who have overstayed from returning again. It would also deter those who fear they may lose the possibility of visiting US relatives from overstaying in the first place (whether or not they work illegally during the duration of their visa is another matter).

Alternatively, if deployment of US-VISIT is not paired with increased enforcement of laws prohibiting employment of illegal migrant workers, visa overstayers who are gainfully employed in the US underground economy may simply opt to remain in the United States and not return home so as to not risk being denied entry. Those who obtain a visa in order to enter the United States and work illegally may opt to stay as well. It may have the same effect that increased enforcement at the US-Mexican border has had—turning temporary illegal migrant workers into permanent illegal migrant workers who opt to have their families smuggled into the United States once rather than paying multiple smuggler's fees and repeatedly risking assault, theft, injury, or apprehension on trips back and forth themselves.

Moreover, with the addition of its biometric capabilities, US-VISIT differs fundamentally from the previous, incomplete automated entry-exit system, which was more susceptible to fraud. With the addition of biometrics, the system has been useful in stopping those with records of criminal or immigration violations from entering the United States, some of whom had previously entered the United States repeatedly using aliases and fraudulent documents but whose fingerprints collected upon entry produced watch list hits in IDENT. By the end of 2004,

US-VISIT was used to arrest or stop 372 criminals and immigration law violators.[48] Moreover, since US-VISIT's biometric capabilities make it more difficult to commit visa fraud, it will most likely deter foreign nationals from attempting it.

With respect to counterterrorism, the DHS has yet to announce the apprehension of a single suspected terrorist with data gathered by US-VISIT. Of course, one can never know how many potential terrorists were deterred. Even if US-VISIT has collected data used to identify a terrorism suspect, law enforcement and intelligence agencies may opt not to make it public, so as not to compromise ongoing investigations. Moreover, the system is not fully developed and deployed. It may be premature to judge the system a failure in achieving the goal of serving as a "vital counterterrorism tool"[49] after only one year's experience with the first increment of the system in place. Nevertheless, even when the system is fully deployed, it is not clear how large a contribution US-VISIT will be able to make to the overall counterterrorism mission.

US-VISIT counterterrorism watch list checks are only as potent as the quality of the intelligence data upon which they rely, the quality of the data US-VISIT collects, and the matching of the two. For example, the DHS inspector general recently concluded that those attempting to enter the United States with stolen passports are usually admitted, that reports of stolen passports on lookout systems made little difference, and that several blocks of stolen passports have been linked to Al Qaeda.[50] After the September 11 attacks, Congress mandated that the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS), which is a ten-fingerprint system, be made interoperable with IDENT. According to a recent Department of Justice Inspector General report,[51] however, "DHS cur-

48 "DHS Entry-Exit System Meets 2004 Goals Ahead of Schedule," Department of Homeland Security, press release, January 2005.

49 *The Intelligence Reform and Terrorism Prevention Act of 2004*, House Report 108-796, Section 7208 (h).

50 "A Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States," op. cit.

51 "Follow-up Review of the Status of IDENT/IAFIS Integration," US Department of Justice, Office of the Inspector General, Report Number I-2005-001, December 2004.

rently plans to use IAFIS to check the fingerprints of less than one percent of the visitors subject to US-VISIT at the ports-of-entry…. Instead, the DHS continues to rely upon the interim measure of checking most visitors' fingerprints against the small portion of IAFIS data extracted into IDENT." The report went on to say that efforts to make the ten-print IAFIS system interoperable with the two-print IDENT system have stalled.

A recent study also found that the two-print IDENT system used in US-VISIT is also susceptible to "US-bound terrorists that have either poor image quality (e.g., worn out fingers) or deliberately reduced image quality (e.g., surgery, chemicals, sandpaper)" because scans from worn fingers reduce the likelihood that US-VISIT would flag a terrorist whose fingerprints are stored on the biometric watch list from 96 percent to 53 percent.[52] A ten-print finger scan system would bring detection rates of worn fingers up to 95 percent, but using IDENT finger scanners to collect ten prints, one at a time (if even possible), could significantly increase the duration of the US-VISIT enrollment process and slow down overall crossing times at ports-of-entry. Replacing the IDENT system and increasing the overall data storage and data handling capacity of US-VISIT may prove to be prohibitively costly for the near future.

In addition to possibilities for system deception, terrorists may simply circumvent US-VISIT by crossing borders between points of entry. One stakeholder in the Detroit-Windsor area noted that while CBP is collecting fingerprints from legitimate travelers crossing the Ambassador Bridge, a terrorist could easily take a boat across the Detroit River into the United States undetected just a few miles up- or downstream, mixing in with Michigan's thousands of recreational boaters. In FY2004, the US Border Patrol apprehended 1.1 million people attempting to cross into the United States between ports-of-entry.[53] For every one

52 Lawrence M. Wein, testimony at the hearing on "Disrupting Terrorist Travel: Safeguarding America's Borders through Information Sharing," US House of Representatives Select Committee on Homeland Security, September 30, 2004.

53 See Immigration Monthly Statistical Report, September 2004 Year End Report, Southwest Border Apprehensions, http://uscis.gov/graphics/shared/aboutus/statistics/msrsep04/SWBORD.HTM.

arrested, it is estimated that several successfully enter. Terrorists could be smuggled into the United States between ports-of-entry, just as hundreds of thousands of illegal migrants are every year. In recent congressional testimony, Deputy Secretary of Homeland Security James Loy noted that new information suggests that "several Al Qaeda leaders believe operatives can pay their way into the country through Mexico (Loy 2005)."[54]

As long as a potential terrorist can steal or purchase a stolen passport and enter the United States "with little reason to fear being caught,"[55] it makes little sense for a terrorist organization to attempt to smuggle its operatives by having them take the dangerous trek through mountains and deserts along the US-Mexican border that most of those smuggled endure due to increased border controls in the more easily traversed urban areas. If a terrorist's travel documents are determined to be stolen or fraudulent upon entry at a US airport, there is a good chance that he will simply be sent back to where he came from on the next available flight, provided that he has not already been identified by the intelligence community as a terrorist suspect and is therefore subject to a warrant for his arrest (with a hold order effectively transmitted to CBP inspectors). If a terrorist were to pose as an illegal migrant laborer who made his way to Mexico and wanted to be smuggled across the border, he would run the risks faced by all smuggled migrants: being robbed, abandoned in the dessert, and possibly dying there, in addition to the risk of being apprehended and deported.

Moreover, the Border Patrol is now using the ten-print IAFIS system in addition to the two-print IDENT system to check those caught crossing the border. Therefore, it would be more likely to uncover terrorists in the law enforcement databases than the current two-print US-VISIT system. The risk calculation for a would-be terrorist is this: "Is it more likely that I will encounter law enforcement entering 'lawfully' at a port-of-entry, or evading law enforcement between ports and then con-

54 James Loy, "Statement of Deputy Secretary Admiral James Loy on The World Wide Threat," US Senate Select Committee on Intelligence, February 16, 2005.

55 "A Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States," op. cit., 3.

tinually evading law enforcement once inside the country?" So far, it seems that terrorists favor the former, but as inspection scrutiny increases at the ports-of-entry, this could change.

Frontline border control officers often compare their task to squeezing a balloon: If you squeeze one end, it expands at the other. Clamping down at one part of the border diverts smugglers and illegal migrants to attempt to cross elsewhere. If one stiffens controls at some ports-of-entry or eliminates one form of visa and document fraud, smugglers will try others and put new pressures on other systems. US-VISIT will increase the risks for terrorists attempting to enter the United States undetected through ports-of-entry. Should they not be deterred and persist in their attempts, US-VISIT may divert them into means of entry that pose higher risks of apprehension and/or other harm that disables them and disrupts their plot.

Essentially, US-VISIT is an additional obstacle to foreign terrorists wishing to enter the United States. However, even when fully deployed, it is unlikely itself to catch many terrorists trying to enter the United States. It is unlikely that "established terrorists" who suspect that they may have been under surveillance will willingly provide the biographical and biometric data that may lead to their apprehension. It is unlikely that the data given by "potential terrorists" who have no criminal record and minimal contacts with terrorist organizations will generate a hit on the watch lists that are checked by US-VISIT. Undeterred, "established terrorists" are more likely to try to circumvent US-VISIT, either by travel document fraud using stolen or fraudulent US or Canadian documents or a fraudulent Mexican border crossing card, or by crossing between ports-of-entry.

There is little that US-VISIT can do to stop the initial entry of an individual who has no record of terrorist-related activities or possible terrorism-related travel (e.g., to Afghanistan in the late 1990s). Once the budding terrorist enters, however, subsequent international travel for meetings (e.g., to counties with active terrorist organizations such as Malaysia) and changes in status (e.g., application for an M visa for enrollment in flight school) may be recorded by the system and raise red flags that trigger investigation. A future terrorist who is smart and well trained may avoid such actions that would raise red flags. Much depends on the intelligence,

experience, and training of the terrorists. As some of the mistakes and risky behavior of some of the 9/11 hijackers indicate, terrorists, much like other criminals, are not always that smart. US-VISIT may succeed in catching a few of the less competent, but there are still simply too many ways to circumvent or deceive the system for it to be much more than a small part of border control authorities' response to international terrorism.

B. Entry process

When US-VISIT went live on January 5, 2004, there were widespread fears that it would slow down incoming visitors at airports and play havoc on connecting flights. The system has performed better than expected. US-VISIT added an average of only fifteen seconds to the entry process and did not significantly impair travel flows at the airports and seaports where it was deployed. By the end of 2004, US-VISIT had processed 16.9 million foreign visitors.[56]

The US-VISIT program completed its Increment 2B rollout at the fifty busiest land border crossings on December 29, 2004, (two days ahead of schedule) and without any appreciable disruptions of traffic flows. It is important to keep in mind, however, that at land borders, enrollment in US-VISIT can be performed in secondary inspection because it is only mandatory for those individuals who require an I-94, and this constitutes only a very small percentage of those crossing land borders.

Enrollment in US-VISIT is only required of those traveling on a regular visa or entering under the Visa Waiver Program. Enrollment in US-VISIT is not required of US citizens, permanent resident aliens, visa-exempt Canadian nationals, or the seven million plus Mexicans with border crossing cards, who together constitute the four largest categories of entries (see Table 1). After the US-VISIT program had been established, it was announced that, for the time being, visa-exempt Canadian nationals[57] would be exempt from mandatory enrollment in

56 "DHS Entry-Exit System Meets 2004 Goals Ahead of Schedule," Department of Homeland Security, press release, January 2005.

57 Canadian nationals entering the United States for short stays are exempt from most visa requirements and also from US-VISIT; however, those who are entering the United States on a visa are required to be enrolled in US-VISIT.

US-VISIT.[58] In response to Mexican objections of unequal treatment in comparison with the United States' other NAFTA partner, the Bush administration decided to exempt Mexican nationals with border crossing cards (so-called "laser visas") that entitle holders to enter the United States and remain in the border region up to twenty-five miles into US territory for up to seventy-two hours.[59] The Border Trade Alliance, a business group representing more than 1,000 industry, government, and education officials, said the plan did not go far enough and advocated that border crossing cards be valid for stays of six months and good for travel throughout the southwest.[60] Stays were extended as of August 12, 2004, but only to thirty days.

Table 1 FY2002 Entries into the United States (in millions) [61]

	Air	Sea	Land	Totals
US Citizens	33.0	7.4	120.7	161.1
Legal Permanent Residents	4.4	0.2	75.0	79.6
Visa Waiver	13.0	0.3	1.8	15.1
Visa Exempt (Canadians)			52.2	52.2
Regular Visa	19.3	4.5	4.5	28.3
Mexican Border Crossing Card			104.1	104.1
Totals	**67.9**	**12.4**	**358.3**	**440.4**

In FY2002, regular visa and visa waiver entries constituted only 6.3 million of the 358.3 million total land border entries, or approximately 1.7 percent. If current entry rates follow recent historical patterns, only 1.5 to 2 percent of those people entering the United States over land

58 "Governor Ridge and Deputy Prime Minster Manley Issue One-Year Status Report on the Smart Border Action Plan," press release, Canadian Embassy, Washington, D.C., October 3, 2003.

59 "US-VISIT Fact Sheet: US Land Borders," http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0371.xml (accessed March 28, 2004).

60 Joe Cantlupe, "Border Group Wants Visa Rules Amended; Proposal Would Aid Mexican Visitors," *San Diego Union Tribune*, April 1, 2004.

61 "Request for Proposals for US-VISIT Program Prime Contractor Acquisition," op. cit., 12.

borders are being enrolled in US-VISIT. Although the challenges of implementing the US-VISIT exit process at land borders are well known, when asked about the exit process, a senior DHS official said, "Exit? I'm not so sure about entry." Upon closer examination, the reasons for this official's skepticism become clear.

The challenge of implementing the entry process of US-VISIT at land borders is evident at the country's busiest border crossing, where there would be a significant impact if the percentage of entries requiring US-VISIT were increased beyond single digits. According to a DHS official, on an average day at the San Ysidro, California port-of-entry, 53,000 vehicles with drivers and 80,000 passengers enter through twenty-four inbound lanes, together with 20,000 to 30,000 pedestrians, for a total of about 150,000 entries. This official flatly stated that if enrollment in US-VISIT took place in primary inspection and added only ten seconds to each individual crossing, it would "kill operations" and lead to unsustainable backups. Similarly, a stakeholder from the Detroit-Windsor area said that the addition of ten to fifteen seconds to the processing of every driver and passenger entering the United States over the Ambassador Bridge would "shut down the bridge."

There were no shutdowns at the end of 2004 when US-VISIT was deployed at San Ysidro and the Ambassador Bridge because enrollment of US-VISIT was accomplished in secondary inspection and required of only a very small percentage of those who entered, and most of these people were already going to secondary for I-94 form processing. There could, however, be very similar negative effects at land borders due to more stringent travel document inspection made necessary by the need to verify the identity of those exempt from US-VISIT (i.e., US citizens, legal permanent residents, visa-exempt Canadians, and Mexicans with border crossing cards). This could happen even without instituting US-VISIT enrollment in primary inspection and maintaining enrollment in secondary inspection at the current enrollment rates.

Upon entry at land borders, US citizens may make an oral declaration of their citizenship, and the inspector, using his or her judgment, may allow the person to enter if satisfied with the totality of information

available or ask to see proof of citizenship (usually a passport). For example, while conducting field research, I crossed both the southern and northern borders. When entering from Mexico through the pedestrian lane at San Ysidro, I pulled out my passport, but the inspector did not look at it; when entering Detroit from Canada as an automobile passenger, the driver told the inspector that we were US citizens, but I was not asked any questions and did not speak, nor were either of us asked for proof of citizenship. In tens of thousands of cases, individuals make false claims to US citizenship. These claims are uncovered when individuals are challenged and cannot produce a valid US passport or other documentary evidence of US citizenship (see Table 2).

Table 2 Apprehensions of Persons with False Claims to Citizenship[62]

	FY1999	FY2000	FY2001	FY2002	FY2003	FY2004
False Claims to US Citizenship	27,781	31,964	30,129	15,293	12,878	12,404
False Claims to other Citizenship	1,108	787	908	836	269	295

Several interviewees from border communities relayed similar experiences to my own as well as recounted the cursory inspection of noncitizens' documents. Technically, CBP officers must visually inspect the travel documents of non-US citizens, but this does not always happen. For example, a US citizen recalled driving into Mexico for one day with two visiting Turkish nationals. When they returned to the United States, the inspector allowed them to enter without asking the driver or his Turkish passengers for their passports.

Those who smuggle migrants though ports-of-entry conduct their own surveillance and know the realities of the inspection processes extremely well. If certain visa fraud schemes and the use of fraudulent foreign passports are foiled by the biometric screening of US-VISIT,

62 Source: INS Form G-22.1.

travel documents that enable individuals to pose as US, Canadian, and Mexican citizens exempt from US-VISIT become much more useful and valuable to smugglers and terrorists. US passports, Canadian passports, and border crossing cards are susceptible to being counterfeited, or genuine documents may be fraudulently altered and used to try to enter the United States, as Table 3 demonstrates.

Table 3 Fraudulent Documents Intercepted at All Ports-of-entry[63]

	FY1999	FY2000	FY2001	FY2002	FY2003	FY2004
Alien Registration Cards	33,295	34,120	26,259	14,373	14,523	16,446
Re-entry Permits[64]	1,107	153	702	1,003	1,193	1,792
Border Crossing Cards	30,797	38,650	30,419	16,265	1,5604	18,587
Nonimmigrant Visas	17,965	17,417	21,127	21,275	19,137	17,934
Immigrant Visas	663	447	597	544	3,309	2,874
Foreign Passports[65]	14,695	15,047	15,994	10,467	6,251	9,041
US Passports[66]	21,196	17,703	18,925	10,892	9,956	12,599
Total Fraudulent Docs	119,718	123,537	114,023	74,819	69,973	79,273

There are 320,000 records of lost or stolen US passports reported since 2002.[67] Anyone can declare his or her US citizenship to avoid US-VISIT. English speakers who have been coached could declare their US citizenship while crossing as a passenger of a vehicle, show the outside cover of an altered US passport if necessary, and, if demanded

63 Source: INS Form G-22.1.

64 and refugee travel documents.

65 and citizenship documents.

66 and citizenship documents.

67 "A Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States," op. cit., 7.

by the inspector, render the altered passport for inspection. Passports with film photographs laminated onto the inside cover are easier to alter with substitute photos than current passports with digital photographs and are therefore much more valuable to smugglers. These older passports were issued until April 2002 and are valid for ten years. Tens of thousands of people attempt to enter the United States with fraudulent US passports each year.

As of September 30, 2004, Canada is the only country whose nationals may enter the United States without submitting any biometrics.[68] There are more than 25,000 Canadian passports reported lost or stolen each year. Although the Canadian Passport Office began deactivating lost and stolen passports beginning in April 2003, the Passport Office did not share its list of deactivated passports with Citizenship and Immigration Canada due to privacy considerations, so inspectors at Canadian ports-of-entry could not identify deactivated passports.[69] As of February 2004, data on lost and stolen passports has been manually entered into Royal Canadian Mounted Police (RCMP) databases,[70] but the March 2004 *Report of the Auditor General of Canada to the House of Commons* notes high error rates and data entry lags.[71] If data on lost and stolen Canadian passports are not also shared with US authorities, Canadian passports stolen in Canada or abroad could be altered and used by individuals to enter the United States without submitting biometrics and without being subject to criminal and terrorist biometric watch lists.

Part of the reasoning for exempting those entering the United States with Mexican border crossing cards is that the border crossing cards contain fingerprint biometrics and a photograph, and the biometric data can be read by swiping the card through a reader. Unfortunately, many US

68 Unless they are legal permanent residents in the United States.

69 "National Security in Canada—The 2001 Anti-Terrorism Initiative," Chapter 3 of the March 2004 *Report of the Auditor General of Canada to the House of Commons*, http://www.oag-bvg.gc.ca/domino/reports.nsf/html/04menu_e.html (accessed March 30, 2004).

70 "Passport Office Responds to Auditor General's Report," press release, #49, Passport Office, Department of Foreign Affairs and International Trade, Canada, March 30, 2004.

71 "National Security in Canada—The 2001 Anti-Terrorism Initiative," op. cit., 31.

ports-of-entry have not had readers, and the biometric inspection has simply been an inspector comparing the photo on the card to the person presenting it.[72] Border crossing card readers were deployed at the fifty busiest land border crossings by the end of June 2004.[73] According to the DHS inspector general, at most of these land ports-of-entry readers were only deployed in secondary inspection and border crossing card holders entering though primary inspection "are unlikely" to have their cards scanned.[74] Hence, "biometric verification" still mostly means inspectors "eyeballing" the photograph on border crossing cards and comparing it to the holder, as interviewees at the border noted. "As a result, the entry of (border crossing card) holders is not electronically recorded and their identity is not verified."[75] Tens of thousands of the border crossing cards presented to inspectors are fraudulent.

In order to ensure that enrollment in US-VISIT is not circumvented by deception, it is necessary that everyone who does not enroll be rightfully exempted. Such circumvention can only be eliminated if those who declare US citizenship are required to present their US passport or other documents to prove it. The Intelligence Reform and Terrorism Prevention Act of 2004 stipulates that as of January 1, 2008, it will be unlawful for US citizens to enter the United States without bearing a valid US passport or other designated documentary proof of citizenship. Similarly, all Canadian and Mexican nationals will be required to present their passports or other proof of citizenship.[76]

---

72 James Ziglar, testimony, "US-Mexican Relations: The Unfinished Agenda," hearing before the Subcommittee on Western Hemisphere, Peace Corps, and Narcotics Affairs of the Senate Committee on Foreign Relations, April 16, 2002.

73 See US-VISIT FAQs: Land Borders, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0447.xml.

74 "Implementation of the United States Visitor and Immigrant Status Indicator Technology Program at Land Border Ports-of-entry," Office of Inspector General, Department of Homeland Security, OIG-05-11, February 2005, p. 17.

75 Ibid.

76 The new law requires "a passport or other document, or combination of documents, deemed by the Secretary of Homeland Security to be sufficient to denote identity and citizenship, for all travel into the United States by United States citizens and by categories of individuals for whom documentation requirements have previously been waived under section 212(d)(4)(B) of the Immigration and Nationality Act (8 USC. 1182(d)(4)(B))," *The Intelligence Reform and Terrorism Prevention Act of 2004*, House Report 108-796, Section 7209 (b).

In order to comply with this legislation, the DHS and State Department have announced the Western Hemisphere Travel Initiative, in which the new travel document requirement will be implemented in phases: by December 31, 2005 for all air and sea travel to or from the Caribbean, Bermuda, Central and South America; by December 31, 2006 for all air and sea travel to or from Mexico and Canada; by December 31, 2007 for all air, sea, and land border crossings. Although US, Mexican, and Canadian passports will be the "document of choice," the DHS and State Department anticipate that the Mexican border crossing card, SENTRI, NEXUS, and Free and Secure Trade (FAST) program cards will serve in lieu of passports.[77]

If inspectors must examine and verify the passports or other proof of citizenship of all the roughly 120 million US citizens that cross land borders, it can easily add ten seconds to the primary inspection of thousands (if not millions) of people at already congested ports-of-entry. Similarly, if all 100 million Mexican border crossing cards must be swiped though a reader to record each entry, or if a one-to-one fingerprint match must be made with the person presenting the card, it could have a similar, if not even more negative, impact on throughput at primary inspection. If inspectors inspected the travel documents of every US citizen, permanent resident, and visa-exempt Canadian national, as well as swiped every border crossing card, the added seconds to the primary inspection process would cause a significant, cumulative increase in average crossing times at many land border crossings. Therefore, in order to minimize the effect on traffic flows at certain border crossings, it may be necessary to add more entry lanes, booths, and inspectors.

There is also a possibility that US-VISIT exemptions for Canadians and Mexicans with border crossing cards could be terminated. In FY2002, visa-exempt Canadian nationals comprised 14 percent of all

77 "New Passport Initiative Announced to Better Secure America's Borders," Office of the Press Secretary, Department of Homeland Security, April 6, 2005 (accessed on April 20, 2005 at: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0652.xml) and "Frequently Asked Questions: Western Hemisphere Travel Initiative" Office of the Press Secretary, Department of Homeland Security (accessed on April 20, 2005 at: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0651.xml).

entries, and Mexicans with border crossing cards comprised 29 percent of all entries. The DHS inspector general expressed "concern" over the exemption of Mexican border crossing card holders, noting "the absence of routine (border crossing card) scanning and lack of exit tracking."[78] The inspector general's report also expressed concern over visa exempt Canadian travelers and noted the interception of eight Canadian citizens at airports between January and August of 2004 who were suspected of terrorist activities. "(B)ecause visa exempt Canadians are not enrolled in US-VISIT, the likelihood of intercepting those same Canadian citizens at land (ports-of-entry) is small."[79] If people in either of these categories were no longer exempt from US-VISIT entry-exit requirements, it would be impossible to direct all those who need to enroll in US-VISIT to secondary inspection, because a shortage of parking space at even the most capacious facilities would lead to gridlock.

As Geronimo Gutierrez, the undersecretary for North America at the Mexican Secretariat of External Relations, put it, "We have pre-NAFTA infrastructure at our borders."[80] With new data collection requirements in addition to increasing trade and travel flows, it may become impossible to process visitors and shipments without backing up traffic unless larger secure areas at border crossings are cleared for inspection lanes and booths and more bridges and tunnels are built, especially between Canada and the United States. Even without the new requirements of US-VISIT, many land ports-of-entry do not have sufficient space for current operations. Indeed, sixty-four ports-of-entry have less than 25 percent of the space they require.[81]

At certain ports-of-entry such as the Detroit-Windsor Tunnel, the busiest passenger crossing on the US-Canada border, there is little space avail-

78 "Implementation of the United States Visitor and Immigrant Status Indicator Technology Program," Office of Inspector General, op cit., p. 17.

79 Ibid, p. 18.

80 Geronimo Gutierrez,"Remarks by Germonimo Gutierrez, Mexican Secretariat of External Relations," North American Integration: Migration, Trade, and Security Institute for Research on Public Policy, Ottawa, April 1-2, 2004.

81 "Data Management Improvement Act (DMIA) Task Force Second Annual Report to Congress," Department of Homeland Security, 2003.

able to expand the number of lanes and booths for secondary or primary inspections. Such physical constraints on expanding existing ports-of-entry, combined with expectations of increasing trade and travel over the coming decades, have led to many proposals for building additional bridges and tunnels between the United States and Canada, particularly at the Detroit-Windsor crossing. These proposals have been thwarted by the dynamics of not-in-my-backyard (NIMBY) interest group politics, the political maneuvering of the privately-held Ambassador Bridge Company, which seeks to build a new span on its own and minimize competition in the meantime, and a lack of political will on the part of state and national governments to raise the taxes necessary to build additional publicly funded bridges. In any event, another crossing is unlikely to be built before 2010, which is not in time to provide increased capacity to handle the increasing throughput demands when all US citizens' documents will have to be checked or if more categories of entries become subject to US-VISIT enrollment requirements.

Implementation of the entry process of US-VISIT at the fifty busiest land ports-of-entry does not appear to have disrupted traffic flows very much. Given prevailing travel document inspection practices and current exemptions from US-VISIT enrollment requirements, however, this has not been a very high hurdle. If the bar is not raised, if entry inspection practices and exemptions do not change, and if no more than 2 percent of those entering must go into secondary inspection in order to be enrolled in US-VISIT, it will most likely be relatively easy to extend the entry process to the remaining land ports-of-entry by the end of 2005 without significant disruptions to cross-border travel flows.

Although it may well be that document inspection practices are now stricter at those land ports-of-entry where US-VISIT has been deployed, this is not clear. In any event, as of January 1, 2008, it will be unlawful for US citizens to enter the United States without bearing a valid passport or other designated documentary proof of citizenship. With all other factors remaining constant, the average time spent in primary inspection by US citizens will necessarily increase, overall throughput will be constrained, and the cumulative impact of US-VISIT on border crossing times will also increase. How much is difficult to say. However, at many ports-of-entry the margin for increase

without leading to backups is very slim. At these crossings, the consequences of implementing US-VISIT over the coming years are potentially very great.

C. Exit process

Congressional mandates refer to an "automated entry and exit process." However, there is not yet much of an automated exit process

Table 4 FY2002 Nonimmigrants Admitted by Mode of Travel at Ports-of-entry That Also Have US-VISIT Exit Pilot Programs[82]

Port-of-entry	Sea*	Air*
Atlanta, GA		987,749
Baltimore, MD		53,569
Chicago, IL		1,397,914
Dallas, TX		596,395
Denver, CO		86,406
Detroit, MI		506,119
Fort Lauderdale, FL		7,066
Los Angeles, CA	2,105	
Miami, FL	53,502	
Newark, NJ		1,298,132
Philadelphia, PA		290,444
Phoenix, AZ		104,428
San Francisco, CA		1,378,394
San Juan, PR		254,031
Seattle, WA		261,350
Totals	**55,607**	**7,221,997**
All ports-of-entry	**338,244**	**24,879,668**

* Excludes the following classes of admission: Crewmen (D1,D2,DX), Expedited Removals (EF,EP,ER), and Visa Waiver Program Refusals (GR,WR).

82 Exit pilot programs announced as of January 1, 2005. Data source: Office of Immigration Statistics, DHS, Supplemental Tables, Table 609, http://uscis.gov/graphics/shared/aboutus/statistics/SupplementalTables.htm (accessed January 4, 2005).

in place. Although biographical exit data are captured from electronic submission of departing airline and ship passenger manifests, a biometrically verified exit process has only been deployed on a pilot project basis at thirteen airports and two seaports since January 1, 2005.

Given that most foreigners entering by airplane and ship most likely leave the country from the same airport or seaport, one can make reasonable estimates from recent entry data as to how many exits are likely to be recorded by the US-VISIT exit pilot programs. If the number of entries in FY2002 were repeated over the course of the past year at Baltimore-Washington International Airport and Miami Seaport, the exits of about 100,000 people were processed with US-VISIT biometric verification. If FY2002 entries levels are repeated at the fifteen ports with US-VISIT exit pilot programs in the coming year, it is likely that the exit of approximately 7 million people will be processed with US-VISIT biometric verification at airports and approximately 55,000 will be processed at seaports. That represents about 29 percent of total expected exits at airports and 16 percent of total expected exits at seaports.

With respect to exit at land borders, in November 2003 DHS staff in charge of inspections referred to the exit process as a "work in progress," with no plans yet for staffing.[83] In March 2004 an official from the US-VISIT program office noted, "Implementation of an exit system at land borders has more complexities and has yet to be determined."[84] In January 2005 the DHS provided more details on the exit process as it announced that it was planning tests for using RFID technology for entry and exit at land borders[85] and in February issued an environmental assessment statement on the Increment 2C proof of concept at the selected land ports-of-entry where it would be piloted.[86]

83 Response to author's question at Customs and Border Protection's Trade Symposium, November 2003.

84 Robert A. Mocny, testimony at hearing on "US-VISIT—A Down Payment on Homeland Security," Subcommittee on Immigration, Border Security, and Claims of the Committee on the Judiciary, House of Representatives, March 18, 2004.

85 "Homeland Security Announces Plans to Test Radio Frequency Identification Technology at Land Borders," Department of Homeland Security, January 27, 2005.

86 *Draft Environmental Assessment, US-VISIT Increment 2C Proof of Concept at Select Land Ports-of-entry*, Department of Homeland Security, February 24, 2005.

At most land border crossings there are currently no facilities for outbound inspections. The existing exit data collection at land borders involves those traveling on visas and under the Visa Waiver Program depositing their I-94 forms in drop boxes when they leave, usually at CBP secondary inspection locations on inbound lanes. At San Ysidro, the Detroit-Windsor Tunnel, and the Ambassador Bridge there was no clear signage on outbound lanes instructing exiting foreigners on where to submit his or her I-94 form. At those border crossings in urban areas, the outbound lanes often have very little, if any, room to pull over and park. A persistent, regulation-obeying individual would have to locate and interrupt a CBP officer to find out what to do with the form, and the most visible officers are those working the inbound lanes. At some crossings into Canada—at the Ambassador Bridge, for example—Canadian inspectors will take I-94 forms given to them and send the forms back across the border to be added to the drop box collection. Contactors then enter the information written on the forms into a database, which can be compared to entry records in ADIS.

According to the US-VISIT request for proposals (RFP), Increment 2B (now called Increment 2C) is also to have a radio frequency (RF) system that captures biographical exit data, and it is to be deployed at one or more land ports-of-entry by June 30, 2005. DHS appears to consider its ability to capture biographical exit data from airline and ship passenger manifests and from a yet-to-be-determined RF system at land borders in pilot projects at five ports-of-entry (Nogales East and Nogales West in Arizona; Alexandria Bay in New York; Pacific Highway and Peace Arch in Washington) to be sufficient to meet congressionally mandated deadlines of the 2000 DMIA. However, from the way in which the entry-exit system has been discussed by members of Congress, it appears that congressional perceptions differ on the meaning of these deadlines and many members expect that a biometric entry-exit system will be in place at all borders by the end of 2005.

In any event, Congress clarified the requirements in December 2004 when it passed legislation that stipulates the following: "The entry and exit data system shall include a requirement for the collection of biometric exit data for all categories of individuals who are required to provide biometric entry data, regardless of the port-of-entry where such

categories of individuals entered the United States."[87] This means that biometric exit data will need to be collected from not only the approximately 37 million people who enter by air and sea with nonimmigrant visas, or under the Visa Waiver Program, but also the six million people who enter over land borders. It also means that those who submit biometrics to US-VISIT when entering by air or sea must also be able to submit their biometrics at land border exits. Therefore, the existing plan to use RF technology to collect biographical data at exit is not sufficient to meet existing legal requirements for the US-VISIT system.

Although there are currently no exit controls at most US land borders, one could envision exit controls at land borders that would mirror entry controls with the construction of additional lanes and booths, the installation of biometric readers and workstations, and the hiring of inspectors to process departing foreigners and record exit data for US-VISIT. The DHS estimated that the cost of infrastructure improvements necessary for the final increment of US-VISIT would be approximately $2.9 billion. This figure, however, assumes that no additional lanes would be required for entry and that exit lane requirements would be the same as those for entry.[88] Given the prospects for increased average crossing times and declining throughput at entry discussed above, this is a rather heroic assumption.

D. Radio frequency-enabled exit controls

The US-VISIT program and the International Civil Aviation Organization (ICAO) have great hopes for using RF technology to expedite travelers through border controls at ports-of-entry. RF-enabled exit controls at land borders that did not include a primary inspection by a DHS officer might save billions of dollars. If US-VISIT were to depend upon RF-enabled exit controls, it might, however, be next to impossible for US-VISIT to achieve its objectives of determining whether someone has overstayed or should be apprehended when leaving because there are limits as to what processes can be securely

87 The Intelligence Reform and Terrorism Prevention Act of 2004, House Report 108-796, Section 7208 (d).

88 Hite, "Testimony for Oversight Hearing: US VISIT—A Down Payment on Homeland Security," op. cit.

automated in the collection of exit data. An RF-based exit system may record the exit of an RF-enabled travel document, but one can only be certain that the person exiting with the document is the same person who entered with that document if that person is physically checked against the picture on the document and the biometrics on the chip.

According to the US-VISIT RFP, "As foreign national travelers leave the United States, their exit will be recorded and, if warranted based on watch list screening results, immediate detainment action will be taken. Entry and exit records will be matched and visa compliance will be determined and maintained along with travel history."[89] The RFP further states, "The Government intends to deploy RF capability at vehicle lanes and use this technology to record biographic entry and exit data for RF-enabled vehicles/passengers."[90] It also states, "The Contractor's exit solution cannot assume that vehicles can be stopped in traffic lanes."[91]

The Increment 3C proof of concept at the five land ports-of-entry proposes to use automatic identifiers (a-IDs) to register exits. When a foreign national enters at one of the 2C pilot land ports-of-entry, he or she will go to secondary inspection to submit biographical and biometric data for I-94 processing and will be issued an a-ID. The a-ID will have a number that is linked to a database with the traveler's biographical and biometric data. No biographical or biometric data are stored on the a-ID itself. The system will then register entries and exits of the traveler with the a-ID when crossing in a vehicle. Pedestrian entry will also include real-time biographic watch list checks. In a second phase of system deployment, a-ID crossings will pull up biographical and biometric data for vehicle primary inspection.[92] In order for such a system to operate, CBP would need to install RF readers over all exit lanes. The RF readers appear to be similar to those used for EZ-Pass and other automated toll systems, some of which now read radio frequency identification (RFID) tags on cars passing by at fifty-five miles per hour.

89 "Request for Proposals for US-VISIT Program Prime Contractor Acquisition," op. cit., 9.

90 Ibid., 118.

91 Ibid., 121.

92 *Final Environmental Assessment, US-VISIT Increment 2C Proof of Concept at Select Ports-of-entry*, Department of Homeland Security, April 13, 2005, 3.

It is hard to envision how an RF system could automatically "check out" holders of automatic identifier cards and RF-enabled biometric passports as they drive through exit lanes and be able to determine whether the person leaving is the same person who arrived. For example, a criminal or terrorist could overstay his visa but be registered as having "checked out" by paying a Canadian national to take his RF-enabled a-ID and exit the United States as a passenger of a car driven through the exit lane into Canada.

To deal with this problem, US-VISIT officials have suggested that a wireless biometric card could be used. As individuals are enrolled in US-VISIT upon entry they would be given an RF-enabled entry-exit card with a wireless fingerprint reader that could transmit a live read of the individual's fingerprint as the person exited so as to verify that the person did indeed leave with the entry-exit card.[93] As drivers and passengers subject to US-VISIT exit requirements cross the land border out of the United States, they would put their finger on the finger scan section of the card as they pass under the RF readers. The reader would collect the data transmitted from the card and the digitized finger scan biometric. The biographical data would be used to register an exit to correspond to the individual's entry and the finger scan biometric would be matched to the finger scan collected upon enrollment to verify the identity of the individual exiting.

Wireless fingerprint readers are becoming increasingly common. They are used in building access control systems, and they are incorporated into the new wireless Microsoft mouse, which is used to verify the identity of a person accessing a computer. Wireless handheld fingerprint readers may be used by CBP inspectors (or contract personnel) to collect biometrics from passengers in the departure lounges of airports and seaports. However, there are no currently available off-the-shelf wireless fingerprint reader cards that are appropriate for the US-VISIT exit process at land borders,[94]

93 As described by Robert Jacksta, executive director, Border Security and Facilitation, CBP, in his presentation "Smart Borders: The Implementation of US-VISIT and other Biometric Control Systems," Alexandria, VA, October 26-27, 2004.

94 This was the information provided by representatives of the biometric industry present at "Smart Borders: The Implementation of US-VISIT and other Biometric Control Systems," Alexandria, VA, October 26-27, 2004.

and operable wireless fingerprint exit verification will have to wait to be part of the final increment of US-VISIT.

Even if such an RF-enabled exit process can be developed, there is a major problem with its practical application. Acquiring a readable fingerprint scan often involves careful placement of the finger on the reader and takes several tries. If the fingerprint is not properly read and transmitted and the exit is not recorded, the departing visitor risks being denied entry to the United States in the future. Moreover, unless there is some way of transmitting a signal that the finger scan has been read and the data received, people may think that their exits were registered when they in fact were not. Airport exit stations provide a paper exit receipt. This would not be the case for an RF-enabled exit process in which vehicles would not stop.

The proposed RF-enabled exit process would also be very susceptible to deception by those who wish to register an exit but then overstay their visas. A finger scan reader on a wireless entry-exit card is much more susceptible to "spoofing" than enrollment in US-VISIT at ports-of-entry. There have been several experiments showing that finger scan readers can be spoofed with fake fingers made of gelatin and other materials.[95] Someone could make a fake finger (following instructions readily available in articles on the Internet) and have someone drive it over the border while pressed on the finger scan reader of the wireless entry-exit card. Antispoofing techniques include supervised enrollment, enrolling several biometric samples, e.g., two fingers instead of one, and multimodal biometrics, e.g., facial and fingerprint.[96] Enrollment in US-VISIT at ports-of-entry employs all three.

Even if a criminal or terrorism suspect attempted to exit without pressing his finger to the finger scan reader or if the RF system registered a

95 See T. Van der Putte and J. Keuning, "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned," *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications* (Kluwer Academic Publishers: 2000); T. Matsumoto, et. al. "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," Proceedings of SPIE 4677 (January 2002).

96 S.A.C. Schuckers, "Spoofing and Anti-spoofing Measures," *Information Security Technical Report* 7, no. 4 (2002), 56-62.

"hit," what could US authorities do if the suspect had already crossed the border into Canada or Mexico, especially if the individual in question held a Canadian or Mexican passport? Are the enforcement measures in this situation as good as what could be attained with an exit inspection process that was similar to the entry process (i.e., presentation of travel documents to an inspector, identity check based on facial recognition and fingerprint scan, watch list check, and optional secondary inspection)?

It is unlikely that a land border exit process in which the automobile does not stop is viable. At best, an automated, self-service exit station could be envisioned. Individuals could drive up to the exit station, then drivers and passengers could use their wireless entry-exit cards to transmit their finger scans to the RF reader. When the exit was recorded, the station would print out paper receipts, and the barrier would lift to allow the car to pass. If the exit generated a lookout hit, the barrier would not rise and CBP officers could pull the vehicle over for secondary inspection. This solution would still be susceptible to deception with fake fingers. The only secure solution would be to require supervised collection of scans of at least two, if not ten, fingers and a digital photo.

As the border community stakeholders who were interviewed made clear, at some border crossings such as the Detroit-Windsor Tunnel, there is little room for secondary inspection of inbound traffic, let alone for secondary inspection of outbound traffic and for additional exit lanes that accommodate primary inspection booths for collection of exit data. Even if only a few vehicles were to be stopped at exit stations, especially at peak traffic times, rows of departing vehicles would quickly back up into the main streets of downtown Detroit. In order to implement a secure exit process, it would be necessary to expand the number of lanes and to build exit booths. However, there are limitations on expanding the physical infrastructure of approaches to bridges and tunnels within the time frame envisioned for the implementation of US-VISIT.

E. Incomplete data, data interoperability, and data availability

Despite the improvements in recording entry data with US-VISIT, the fundamental problem of the previous, partially deployed entry-exit system remains. A tracking system cannot determine who is in the country if the data are not complete. If data are not collected on every entry and corresponding exit, the database will not be complete and subject to persistent errors.

Given the obstacles of collecting biographical and biometric exit data at land border crossings and the large costs it may entail, it is understandable why border community stakeholders fought exit data collection requirements before September 11, 2001. It is understandable why policymakers opted to exempt Canadian nationals and Mexicans with border crossing cards from US-VISIT enrollment requirements and why policymakers may opt to delay full implementation of US-VISIT exit data collection at land borders. However, if records generated by the entries and exits of all visa holders and nationals of Visa Waiver Program countries as well as all Canadians and all Mexicans are not somehow captured by US-VISIT or fed into US-VISIT in compatible formats by other reliable information systems, it is unlikely that US-VISIT will function like the entry-exit system envisioned by Congress and mandated by law.

US-VISIT is like an inventory tracking system of a warehouse with 326 doors. Records of items may be generated through manual data entry at the loading dock or with barcode scans or with RFID systems. If you want an accurate report on what items came into and left the warehouse during the previous year as well as how many items are in the warehouse at any given time, data on all items need to be entered into the system. If, for example, all items from one vendor, Maple Leaf Widgets, came into the warehouse but were not entered into the system, the database would be inaccurate, even if most of those items eventually left the warehouse. If Maple Leaf Widgets is one of the largest vendors shipping to the warehouse and its items are exempted from data entry requirements, that makes for a very ineffective inventory tracking system regardless of how good the hardware and software may be.

There is an old saying in computer programming that applies to the scenario presented above: nothing in, nothing out (NINO). Just as an inventory tracking system cannot track items whose data have not been entered into the system, US-VISIT will be unable to track all those who enter and leave the United States unless all of their data are entered into the system. Currently, the situation with US-VISIT is as if there are some 440 million items entering the warehouse each year with only 45 million of those items being registered in the system. Most of those 45 million items (though still an uncertain number) will be recorded in the database when they leave the warehouse, but the majority of those records are based on shipping manifests. Only seven million exit records are actual barcode scans of the items as they leave through one of the 326 doors.

Since the first increment of US-VISIT is comprised of the above-mentioned legacy systems and is not a comprehensive system, it lacks interfaces with the databases that contain biographical and biometric data of Mexican nationals with border crossing cards as well as data collected from those enrolled in the NEXUS and SENTRI programs.[97] Even if interfaces are built between these legacy systems, the absence of preexisting data standards may preclude adequate data sharing between US-VISIT, the border crossing card databases, NEXUS databases, and SENTRI databases.[98] That is, the same data objects in individual existing systems may have different names, and different data may have similar or the same names. The format of data fields may vary across systems, and due to memory limitations, older legacy systems often use alphanumeric "smart numbers" with specific digits to designate attributes of particular data objects, whereas newer systems generate sequential or random item numbers and have more data fields for item descriptors.

In addition to building interfaces, data interoperability often requires normalization of large volumes of master data and the building of translation tables. Therefore, even if data are collected from enrollees

97 Author's discussion with DHS official, April 9, 2004.

98 See "Data Management Improvement Act (DMIA) Task Force Second Annual Report to Congress," op. cit., 124-137; "Final As-Is Enterprise Architecture Description," US Department of Homeland Security, July, 16, 2003, 22-26.

in the border crossing card, NEXUS, and SENTRI programs, and even if these programs require collection of even more data than is gathered by US-VISIT, the contents of these databases are not necessarily immediately useable for an entry-exit system.

These data can be normalized and data standards can be set for new data entered into systems. However, getting several agencies, departments, and programs within any given organization to agree on a set of data standards is often very difficult because users of any individual system usually want to keep their existing data formats, customer numbers, codes, etc. rather than adopting others. Setting data standards usually requires ongoing discussions within program-spanning data standards groups that have backing from high-level management to enforce new standards on recalcitrant system users.

The DHS Standards Portfolio in the Science and Technology Directorate has been addressing the standard setting involved in the merger of twenty-two agencies into DHS, and there are working groups examining standards for biometrics and RFID.[99] Both groups deal with critical components of US-VISIT, and such standards groups could play a critical role in establishing data interoperability among the currently interfaced systems making up US-VISIT as well as additions such as the border crossing card, NEXUS, and SENTRI databases. Success will depend, however, upon the level of cooperation that data standard groups receive from individual program managers as well as the support provided by top DHS management if such cooperation is not forthcoming.

As the system is deployed in more ports-of-entry (and exit) and as time goes by, the amount of biographical and biometric data stored by US-VISIT's component systems will accumulate. This will be magnified if Canadians and Mexicans are also required to enroll and if the volume of international travel to the United States increases.

---

99 Bert M. Coursey, "Science and Technology Directorate Standards Portfolio: Challenges, Needs and Priorities in Homeland Security," presentation to American National Standards Institute, October 1, 2003, http://web.ansi.org/meetings_events/featured_events/wsw03/agenda03.aspx?menuid=8 (accessed December 5, 2004).

Since entry data must be saved and made available upon demand to match with exit data, and since it will be necessary to archive entry-exit records in order to establish travel patterns and determine anomalies as well as to conduct potential future investigations into travel patterns of suspects, there will be tremendous data storage capacity requirements.

Moreover, to be useful, these data and the data management systems must be available twenty-four hours a day, seven days a week, 365 days a year and provide real-time response to queries by inspectors or other officials. The Government Accountability Office (GAO) has pointed out that the technical performance measures (e.g., system availability, timeliness, and output quantity) have been defined for Increments 1 and 2B, but other performance measures for reliability, resource utilization, and scalability have not. The GAO has also noted that it is not clear from current documentation to what degree US-VISIT relies on "existing systems that have less demanding performance requirements such as the 98 percent availability of the Treasury Enforcement Communications System."[100]

F. RF technology and Visa Waiver Program country passports

Increment 2A of US-VISIT was to deploy equipment and software at all ports-of-entry to capture biometric data from machine-readable travel documents by October 26, 2004. The deadline was extended because even if a Visa Waiver Program country incorporated biometrics on contactless IC chips into its passports in time, CBP officers at US ports-of-entry might not have had the right equipment to read the data from those passports. Until recently, there was no agreed-to international standard for guaranteeing interoperability of contactless IC chips and RF readers. Different radio frequencies are used by different companies that make RF systems, and if countries in the Visa Waiver Program began purchasing these systems before a single RF standard was agreed to, the IC chips in some passports might not be readable by the machinery at the US port-of-entry, or the United

100 GAO, "Some Progress Made," op. cit., 6.

States might have to invest in as many as twenty-seven different readers for all of the different passports.[101]

After the March 22–April 2, 2004 meeting of the ICAO Facilitation Division, ICAO revised the standard to address this interoperability problem. The ICAO New Technologies Working Group produced a technical report that recommends IC chips conform to ISO standards ISO/IEC 14443 Type A or Type B.[102] Since the standard was approved in May 2004, that left only five months for Visa Waiver Program countries to deploy new passports with RF chips and five months for the United States to install the RF readers that are compatible with those passports at all US air and sea ports-of-entry. Given this very short time frame, former DHS secretary Ridge asked and received an extension of the deadline from Congress for the DHS to install equipment for biometric comparison and authentication of passports.[103] According to Elaine Dezenski, readers will not be in place at all ports-of-entry by October 26, 2005, the current deadline for Visa Waiver Program countries to issue RF-enabled biometric passports.[104]

Another potential problem for readers of RF-enabled biometric visas and passports has emerged in the European Union (EU). EU member states all agreed to issue passports with both facial and fingerprint biometrics on ICAO compliant IC chips, and they have agreed to issue RF-enabled biometric visas. An EU technical expert group has reported that a "problem of collision" may arise when there are several RF-enabled visas affixed to an RF-enabled passport, each transmitting their own data to the reader, creating interference and leading to sys-

101 Response to author's question on a presentation at the event "Entering America: Challenges Facing the US-VISIT Program," Heritage Foundation, March 1, 2004.

102 ICAO, "Biometrics Deployment of Machine Readable Travel Documents," ICAO TAG MRTD/NTWG Technical Report Version 2.0, May 21, 2004.

103 Tom Ridge, "Testimony of Tom Ridge, Secretary of the Department of Homeland Security, before the House Committee on the Judiciary, April 21, 2004."

104 Answer to question asked of Elaine Dezenski, Acting Assistant Secretary, Border and Transportation Security Directorate, Department of Homeland Security, before the Judiciary Subcommittee on Immigration, Border Security and Claims of the House of Representatives, April 21, 2005.

tem malfunction.[105] US-VISIT RF readers at US ports-of-entry may encounter a similar problem of collision when nationals of states with ICAO compliant RF-enabled passports travel to the United States through one or more EU members that affix RF-enabled visa stickers to passports. US-VISIT readers may encounter difficulties reading EU member state passports that have RF-enabled visas affixed to them as more and more states adopt RF technology for their visas.

The original thinking behind exempting nationals of Visa Waiver Program countries from US-VISIT enrollment requirements was that they would have RF-enabled passports with biometrics that could verify the bearer's identity at the port-of-entry. If, by the new deadline in October 2005, at least some Visa Waiver Program countries issue their biometric passports, it stands to reason that nationals of those countries should no longer need to be enrolled in US-VISIT. On this question, the US-VISIT Web site states, "The Departments of Homeland Security and State will continue to review and analyze any additional changes that might need to be made and will make considerations at the appropriate time and with all of the appropriate inputs."[106] The Department of Homeland Security inspector general, however, recommended that nationals from Visa Waiver Program countries continue to enroll in US-VISIT even after they have RF-enabled biometric passports. The US-VISIT office responded to this recommendation with: "We agree. The Department has stated that it will continue enrolling and processing VWP travelers through US-VISIT, even after the ICAO-compliant passports can verify that passports and the readers to use them are in place. While biometric passports can verify that the passports are genuine, they do not provide capability for biometric watchlist checks."[107]

105 Council of the European Union, "Technical feasibility of the integration of biometric identifiers into the uniform format for visa and residence permits for third country nationals, passports and other travel documents issued by Member States," Committee Report 14534/04, LIMITE, VISA 203, COMIX 684, Brussels, 11 November 2004.

106 "US-VISIT FAQs: Visa Waiver Countries." http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0443.xml (accessed January 2, 2004).

107 "Implementation of the United States Visitor and Immigrant Status Indicator Technology Program," Office of Inspector General, op. cit., p. 28.

Given the implementation difficulty that the EU is anticipating with readers for its own RF- passports and visas, it is not clear that US-VISIT will be able to effectively collect data from these passports. Moreover, older passports issued by Visa Waiver Program countries before the issuance of new RF-enabled biometric passports would still be valid, and it is unlikely that the DHS would agree to stop requiring enrollment in US-VISIT of those holding such older passports. The US-VISIT program has also become the primary program for watch list checking. Since ICAO-compliant passports of Visa Waiver counties will not necessarily contain fingerprint information, but will include digital photographs, the biometric component will not be well suited to watch list checks, which rely on fingerprint data. Before September 30, 2004, there was a discrepancy between Visa Waiver Program countries whose nationals were not required to submit fingerprints and all other states.[108] This became a diplomatic sore point with certain countries that considered it a double standard, especially Poland. It would be very difficult for the DHS to return to the previous status quo and stop requiring the collection of fingerprints from Visa Waiver Program county nationals if they carried ICAO-compliant passports that only included facial biometrics.

The EU, however, has agreed to a standard requiring all member states to include fingerprints in their new ICAO-compliant biometric passports. Even if the EU includes fingerprints in its passports, however, plans call for only two fingerprints, as opposed to existing US law enforcement fingerprint databases based on ten prints. Again, this presents the same problems of interoperability between IDENT and IAFIS and potential security gaps inherent to a two-fingerprint system. As he was leaving office, former DHS secretary Ridge recommended to his successor that US passports include ten fingerprints.[109] This may be an indication of the direction for US standards, not only for US-VISIT but also for all passports. If so, EU member states will have an even higher standard to meet in order to maintain visa-free travel and

108 See Rey Koslowski, "International Cooperation on Electronic Advanced Passenger Information Transfer and Passport Biometrics," ISA, Montreal, March 17-20, 2004, http://tecn.rutgers.edu/politicalscience/koslowski.html.

109 Answer to question posed after former DHS secretary Ridge's presentation at the Center for Strategic and International Studies, January 12, 2005.

eliminate the US-VISIT enrollment requirement. For all of these reasons, it is doubtful that the current US-VISIT enrollment requirement for nationals of Visa Waiver Program countries will be lifted in the near future, if at all.

G. A world of digitized biometrics

Beyond the physical infrastructure and data acquisition problems associated with the implementation of biometric entry-exit systems, there are certain data security problems with the use of biometrics. For example, computer security experts point out that biometrics are unique identifiers, but they are not secrets. Further, biometric security systems also do not "handle failure well."[110] Finger scans are being increasingly used instead of passwords for access to personal computers and networked systems. If, for the sake of argument, a criminal (or terrorist) stole someone's digitized fingerprints, and the victim's computer system used fingerprint biometrics for remote access control, that criminal could potentially access the system. Worse yet, once the person's fingerprints are stolen, he or she cannot get new ones in the way that he could simply change his or her password. Moreover, the security breach is compounded if fingerprint biometrics are used by additional systems (e.g., the person's online banking account). Unlike password-based security (in which you can use different passwords for different systems), once the digitized biometric is stolen, all systems that use it are compromised and a person might not be able to use that biometric in future authentication systems.

US-VISIT already has a database of more than 16 million fingerprint scans and the number will most likely increase dramatically over the coming decade. Brazil is the only country that has so far imposed reciprocal requirements for the collection of biometrics from US citizens, but it is naïve to think that other countries will not follow suit, especially after the initial technology development costs are absorbed in the first implementations and copies of US-VISIT–like systems become available on the world market at declining prices. Senior DHS

110 Bruce Schneier, "Biometrics: Uses and Abuses," Inside Risks 110, *Communications of the ACM 42*, no. 8 (August 1999).

officials have noted that there are other countries developing programs like US-VISIT and welcome this.[111] As more and more countries develop US-VISIT–like entry-exit systems and more and more people submit their biometrics while traveling, databases will soon be filled with hundreds of millions of digitized fingerprints. At some point, the digitized biometrics of the vast majority of the world's international traveling public will be in the databases of the immigration and border control authorities of many countries.

The existing US-VISIT system may have robust physical and database security,[112] but what about the rest of the world? How secure will all of the world's digitized biometrics be from theft? What if a human smuggling organization or a terrorist organization were to acquire files with the biographical and biometric data of thousands, if not millions, of travelers, including US citizens? These files could prove useful for identity theft and credit card fraud, for gaining access to biometrically accessed computer systems, and for visa and travel document fraud. Such a breach of database security could not only enable widespread theft and the commission of crimes under assumed identities, but it could also facilitate terrorist travel around the world.

Perhaps even more damaging to the US-VISIT program itself, a database security failure in any US-VISIT–like system in any country would undermine the confidence in the data protection provided by government systems and most likely precipitate a revolt among those people who previously were willing to voluntarily submit biometrics to government agencies. Moreover, much as the theft of one's digitized fingerprints would compromise a biometric-based verification system used to gain access to a computer, if the security of large amounts of biometric data were compromised by terrorists, it could call into question the use of those biometrics in many authentication systems, perhaps even the utility of continuing to collect biometrics by border control agencies. Nothing demonstrates success like emulation. Yet if US-VISIT were to be widely imitated, inadequate database security

111 Ridge, "Testimony before the House Committee on the Judiciary," op. cit., 4.

112 "US-VISIT Program, Increment 2 Privacy Impact Assessment," Department of Homeland Security, September 14, 2004.

beyond the control of US authorities could pose risks to the utility of the biometrics, into which so much effort and expense went in the first place.

V. RECOMMENDATIONS

A. Reconsider policy and/or revise implementation expectations

Based on current deployment limitations, the implementation challenges still to be addressed, the uncalculated costs for necessary border infrastructure, and the risk that the system, even when fully deployed, may not achieve the counterterrorism objectives envisioned, the Bush administration and Congress should consider reassessing their commitments to the US-VISIT program.

If counterterrorism is the primary justification for the system, the administration and Congress should reconsider the opportunity costs of US-VISIT deployment in relation to spending on other initiatives and programs dedicated to disrupting terrorist travel such as improving information sharing on stolen passports, better incorporation of stolen passport data into watch lists, intelligence programs to better identify travel document fraud associated with terrorists, and other intelligence measures.

If counterterrorism is not the primary justification but reducing visa overstayers is, then the administration and Congress should consider the opportunity costs in relation to spending on other forms of immigration law enforcement. Given that most visa overstayers remain in the United States in order to work, investing several hundred million dollars in developing an employment eligibility verification system may enable effective internal enforcement of immigration laws, dry up demand for illegal migrant workers, and reduce the number of visa overstayers much more effectively and economically than implementing US-VISIT.

If after such a policy reassessment of the opportunity costs of the US-VISIT system, the administration and Congress continue to support the US-VISIT program, they should commit to a full deployment of a complete system that registers all entries and exits, including those of all US citizens, Canadians, and Mexicans. The system should be highly scalable, and there should be an overabundance of data storage capacity built into the planning and funding of the system—sufficient to store entry and exit data of all 450 million people who enter annually and to accommodate ten fingerprints of all of these people, if deemed necessary. An incomplete system that only enrolls a small fraction of entries and an even smaller fraction of exits is too easily circumvented by terrorists and human smugglers alike. It may provide a way for policymakers to reassure the public and demonstrate they are doing something to combat terrorism and illegal migration, but a partially deployed US-VISIT system will not be effective in accomplishing its intended missions. If the president and Congress are not willing to expend the political capital and budgetary resources necessary for full implementation of US-VISIT, it may be better not to develop it at all.

B. Use technology appropriate to the task

US-VISIT should remain one tool among the many used by CPB inspectors to screen for terrorists, criminals, and immigration law violators. In congressional hearings on US-VISIT, Robert Jacksta, executive director of Border Security and Facilitation, CBP Office of Field Operations, stated, "We do train our inspectors in a number of areas—document fraud, interviewing techniques—and that training is important to make sure that we have a layered approach. We don't count on one specific type of tool to identify individuals. We bring it all together so that we can respond appropriately."[113] However, there is the old saying that when the only tool you have is a $10 billion hammer, everything begins to look like a nail.

DHS must resist letting US-VISIT become the answer to an increasing range of homeland security problems for which it may not be the opti-

113 Robert Jacksta, answer to question posed at a hearing of the Committee of the Judiciary, Subcommittee on Immigration, Border Security and Claims, March 18, 2004.

mal tool. This becomes especially tempting as US-VISIT becomes a big budget item that needs to be justified before Congress every year. Moreover, if inspectors increasingly use US-VISIT to make their determinations, a negative feedback loop could develop in which inspectors become overly dependent on biometric scans and automated watch list checks and fail to develop or retain interviewing and document inspection skills. This negative feedback loop could lead to deterioration of human capital in frontline CBP positions in the same way that US intelligence became increasing dependent on satellite imagery over the past decades and human intelligence capabilities deteriorated—to disastrous effect.

C. Hire more inspectors

Congress and the administration should consider authorizing DHS to hire additional inspectors at ports-of-entry in order to maintain a balance between spending on information technology and human resources. DHS officials often describe technology as a "force multiplier" that can be used to counter terrorism.[114] Many organizations in both the public and private sectors have used similar concepts in arguments for spending on information technology in lieu of hiring new staff or to reduce staff size through automation. US-VISIT deployment should not be considered a "force multiplier" of the existing CBP inspectors that in any way should be considered a substitute for more inspectors.

The Intelligence Reform and Terrorism Prevention Act of 2004 authorizes increasing the number of full-time Border Patrol agents by 2,000 per year for five years and increasing the number of full-time Immigration and Customs Enforcement investigators by 800 per year for five years, but it does not specifically authorize increasing the number of CBP inspectors at the ports-of-entry. Moreover, the Bush administration has indicated that it will be asking for funds to hire only 210 of the 2,000 authorized additional Border Patrol agents in FY2006,[115] noting that it is more important to fund purchases of technology such

114 Tom Ridge quoted in Murphy 2002.

115 "Budget in Brief, Fiscal Year 2006," DHS, 27.

as sensors and cameras.[116] Moreover, there is anecdotal evidence that many of the most experienced CBP inspectors are being hired by other agencies due to differences in labor contracts and wage scales across the DHS and federal law enforcement agencies.

Congress and the president should consider hiring and training more CBP officers at the ports-of-entry in order to meet increasing demand resulting from the need to physically inspect all travel documents at land borders. If one of the easiest ways for a terrorist to enter the United States is to simply declare US citizenship and have a stolen US passport available for proof of citizenship if contested, then CBP should ensure that all travel documents are as carefully inspected at land borders as they are at airports and seaports. It would be just as easy, if not easier, for a terrorist with a stolen US passport to fly to Tijuana instead of San Diego or Windsor instead of Detroit, and then cross the land border into the United States as a pedestrian or a passenger of a car or bus.

Table 5 Border Control Agency Staffing

Country	Land borders (miles)[117]	Staff (approx.)	Staff/mile
United States	7,521	41,000	5.5
Germany (total)	2,263	40,000	17.7
Germany (non-Schengen)[118]	688	40,000	58.1
Poland	1,742	16,000	9.2
Hungary	1,357	11,000	8.1

With respect to staffing, a bit of international comparative perspective may be useful. Table 5 provides a rough comparison of US Bureau of Customs and Border Protection staffing with that of several European

116 Tom Ridge quoted in Hall 2005.

117 CIA Fact Book, http://www.cia.gov/cia/publications/factbook/index.html.

118 Only 688 miles of Germany's borders (with Poland and the Czech Republic) are external Schengen borders that are patrolled and have border crossing checkpoints. Internal borders among parties to the Schengen Convention are lifted as they enforce a common external border.

countries. CBP staffing is quite modest compared to border control agencies of other advanced industrialized countries with large-scale immigration flows such as Germany, especially in relation to the length of their respective land borders.

CBP has 40,828 employees,[119] of whom 10,739 are Border Patrol agents[120] and 18,000 are CBP officers at ports-of-entry.[121] This is roughly equivalent to the size of Germany's *Bundesgrenzschutz* (Federal Border Police) with 40,000 employees (30,000 of whom are officers, with 21,000 stationed at border crossing points).[122] Poland has 16,000 border guards and will hire 5,300 more by 2006.[123] In 2001, Hungary had 11,000 border guards and planned to increase the total to 14,000.[124]

D. Use port modeling and simulation to better phase in system deployment

If the president and Congress commit to complete implementation of US-VISIT, the DHS should develop port models and simulations of all 326 ports-of-entry in order to plan US-VISIT deployment and related policy changes so that negative repercussions are minimized. The US-Canada Smart Borders Declaration calls for "border modeling exercises,"[125] and the annex to the 2003 DMIA report uses high-level modeling of the border management process and provides a rationale for

119 "Budget in Brief, Fiscal Year 2006," DHS, op. cit., 23.

120 Ibid., 27.

121 See Deborah Waller Meyers, "One Face at the Border: Behind the Slogan," draft manuscript, Migration Policy Institute, February 17, 2005.

122 Although roughly comparable, the *Bundesgrenzschutz* is not composed of the same array of functions as the CBP in that it also includes the Federal Railway Police (the US counterpart would be Amtrak Police), but it does not include customs inspectors, which CBP does. See *"Grenzschutz Aufgaben"* at: http://www.bundesgrenzschutz.de/Aufgaben/index.php.

123 William J. Kole, "EU expansion to isolate poor neighbors," Seattle Times, April 11, 2004.

124 See EU Enlargement, Hungary 2001 Regular Report, http://europa.eu.int/comm/enlargement/report2001/.

125 "19) Infrastructure Improvements. Work to secure resources for joint and coordinated physical and technological improvements to key border points and trade corridors aimed at overcoming traffic management and growth challenges, including dedicated lanes and border modeling exercises," *US-Canada Smart Borders Declaration*, White House 2002a.

modeling and simulation for systems development.[126] The General Services Agency (GSA), Federal Highways Administration (FHWA), CBP, and ICE developed a computer-based model called "Border Wizard" that simulates cross-border movements of vehicles and pedestrians as well as all federal inspection activities at any land port-of-entry. Maintained by GSA, Border Wizard has been used by more than sixty ports-of-entry for infrastructure project evaluation, and CBP has used Border Wizard to evaluate inspection processes.[127]

The US-VISIT office and CBP should extend and expand their port modeling with Border Wizard by simulating US-VISIT implementation at all ports-of-entry—air and sea, in addition to land.[128] DHS should develop models of existing traffic and passenger flows within existing infrastructure, staffing, and policy constraints to serve as a baseline for simulations. Then, simulations could be run by changing individual or multiple parameters such as the introduction of new policies (e.g., requiring Mexican border crossing card holders to enroll in US-VISIT) and then measuring the changes in throughput.

Many arguments for and against US-VISIT cite projections of the effect of US-VISIT on cross-border flows, but these projections are highly speculative. They also are not necessarily grounded in the particularities of the ports in question. Using modeling and simulation, DHS could gain a better understanding of the likely impact of US-VISIT on the throughput at each individual port and enable policymakers to plan accordingly, whether in terms of staffing, building infrastructure, or scheduling system implementation or policy changes. Individual port models could be incorporated into regional or even national models,

126 "Any attempt to construct a complex system should use modeling as a tool to clarify the major goals and intended uses of the system. A model is a preliminary pattern serving as the plan from which an item not yet constructed will be produced. Models are representations and simplifications of reality, and users must apply practical judgment. Modeling the major concepts and their relationships assists in analyzing the problem domain. Multiple models describe static structures, dynamic behavior, technology usage, and product packaging constraints. With high-level models, a simplified mental model of the problem of border management emerges," *The Data Management Improvement Act* (DHS 2003: Annex 23).

127 See "Border Wizard," Federal Highways Administration, Research and Technology, http://www.fhwa.dot.gov/rnt4u/ti/border_wizard.htm.

128 A DHS official has confirmed that the US-VISIT office is modeling ports-of-entry.

which would be useful in system-wide planning of border infrastructure investments such as building new bridges.

Even more importantly, a national model would enable DHS to simulate the system-wide effects of an attack that shuts down one or more ports; draw up contingency plans for rerouting traffic, shipping, and flights; and build surge capacities sufficient to handle rerouted traffic. If policymakers and stakeholders had a more accurate picture of the impact of US-VISIT on cross-border flows, they could better plan and raise funds for the infrastructure and staffing necessary for effective implementation of US-VISIT. If policymakers could demonstrate realistic plans for dealing with a wide range of possible constrictions of traffic flows and other contingencies, implementation of US-VISIT might not appear as daunting to the business community, and this may help US-VISIT gain its acceptance, if not support.

E. Explore alternative inspection options

The physical limitations of US-VISIT implementation imposed by deficient land border crossing infrastructure, particularly at bridges and tunnels in binational urban areas, may be partially overcome by intensified international law enforcement cooperation. Instead of building exit booths and staffing them with CBP officers to conduct primary exit inspections, Canadian border control officers could simultaneously conduct their entry inspections together with US exit inspections, so-called "reversed inspections." Canadian officers would collect biographical and biometric data and enter that exit data into US-VISIT.[129]

Canada and the United States have already shared in infrastructure development at two ports-of-entry (Oroville, Washington, and Sweetgrass, Montana) and have agreed to a land preclearance pilot project at the Buffalo-Fort Erie Peace Bridge that will move all US primary and secondary inspections to the Canadian side of the bridge. A similar reversed inspection arrangement could be envisioned with Mexico. However, Mexican immigration authorities do not inspect all

129 This had been recommended in the DMIA Task Force's first Report to Congress (INS 2002), 37.

vehicles and individuals crossing into Mexico from the United States at land ports-of-entry, but do so further in the interior. For Canadian and Mexican officials to assume responsibility for the US-VISIT exit process, it would require significant cost sharing and a high level of mutual trust. Nevertheless, it may be the best, if not the only, secure option short of building and staffing an exit infrastructure comparable to the existing entry infrastructure.

Another alternative would be to move inspection areas away from border chokepoints several miles into Mexico, the United States, and Canada. As Stephen Flynn proposes, inspection processes can be moved away from borders to trilateral inspection facilities on dedicated, secure corridors leading to the border.[130] Such trilateral solutions, however, would require even deeper cooperation.

F. Initiate national debate on fingerprints in US passports

Congress should initiate a national debate on the inclusion of fingerprints in US passports. Congress has had little difficulty voting unanimously for legislation requiring the submission of biometrics from foreign nationals, but has been mute on the question of requiring biometrics from US citizens. The State Department began a program to develop new US passports with digital photos on IC chips on its own accord without a congressional mandate. The fact that US citizens are not subject to the same biometric requirements as non-US citizens is not simply an issue of fairness. The issue is whether or not, regardless of US legislation, implementation of the US-VISIT fingerprint requirement will lead to US citizens submitting their fingerprints in order to travel internationally.

It is naïve, if not irresponsible, to expect that other governments will not reciprocate, like Brazil, and eventually require the same biometrics of US citizens that the United States requires of their citizens. As more countries adopt reciprocal visa policies and entry requirements, finger-

130 Stephen E. Flynn, "The False Conundrum: Continental Integration vs. Homeland Security," in Peter Andreas and Thomas J. Biersteker, *Rebordering of North America: Integration and Exclusion in a New Security Context* (London: Routledge, 2003).

prints will be collected from a larger percentage of those US citizens who travel abroad. US officials who desire such biometric collection for security purposes may achieve their objectives by having the requirement imposed by other governments rather than by taking the more politically difficult, but more honest, route of openly advocating legislation. Since the imposition of fingerprint requirements on US citizens by other countries would only be a response to US-VISIT requirements imposed on their nationals, the US government should not require submission of any biometrics of foreign nationals that the US public is itself not prepared to submit.

Former DHS secretary Ridge has said that he will recommend to his successor that US passports include ten fingerprints,[131] and he should be congratulated for finally putting the issue on the table. It is now up to Congress and the president to debate this issue and come to a policy decision. If Congress and the president do not pass and enact legislation requiring fingerprints in US passports, then Congress should pass legislation dropping the requirement of fingerprints for enrollment in US-VISIT.

G. Ensure database security

DHS should ensure that the databases containing biographical and biometric data collected by US-VISIT are extremely secure so as to minimize the risk that biographical data (such as date and place of birth) and digitized biometrics are not stolen by identity thieves or terrorists. The US-VISIT office has developed a security plan that explains the controls that are in place or are planned and states that a security risk assessment in accordance with National Institute of Standards and Technology (NIST) guidelines will be conducted. However, the risk assessment has not yet been completed, and there is no deadline set.[132] Given the potential far-ranging ramifications of a US-VISIT database security breach, the risk assessment should be completed as soon as possible, and any major database security risks

131 Answer to question posed after former DHS secretary Ridge's presentation at the Center for Strategic and International Studies, January 12, 2005.

132 "Some Progress Made," GAO, op. cit., 52.

should be expeditiously addressed with appropriate measures. It would be much better to plug the database security gaps before the amount of biographical and biometric data begins to increase at even greater rates, as more data are collected by US-VISIT and as its deployment is expanded. Given that a future database security breach in another country could have a blowback effect in the United States and undermine the confidence of travelers and citizens in automated entry-exit systems worldwide and in US-VISIT itself, the DHS should also offer to assist other governments with data security.

VI. CONCLUSION

The entry-exit tracking system that became US-VISIT began as a system to help enforce immigration law by identifying visa overstayers, but then was promoted as a counterterrorism tool after the September 11 attacks. Despite huge expectations and relatively large costs, US-VISIT can only be a small part of the country's defenses against terrorism. Since "established" terrorists are unlikely to voluntarily submit their biographical and biometric data, and "potential" future terrorists are unlikely to have records in watch lists, US-VISIT is unlikely to catch many terrorists. At best, it may deter some terrorists and deflect the more determined to make more difficult clandestine crossings between ports-of-entry.

Installing a system and software is not enough to make borders totally virtual. Physical border infrastructure investments as well as accurate, complete, and interoperable data are necessary for the system to work properly. In order to ensure security, more inspection personnel also will be required for adequate inspection of travel documents of those who are not enrolled in US-VISIT and to monitor the biometric enrollment of those who are.

Do US-VISIT's potential benefits justify the necessary investments in border infrastructure, data acquisition, and human resources? Are the

president and Congress willing to expend sufficient political capital to overcome these barriers? If the answer to the second question is "yes," then Congress must work with the DHS to identify and fund critical border infrastructure improvements, pass laws that will ensure complete data (i.e., enrollment of all who enter and exit the United States, including US citizens), appropriate funding for a sufficient expansion of CBP and US-VISIT program personnel, and raise sufficient revenue to pay for all of it. The president must lead by advocating tax increases or borrowing to fund the program and assertively clear local obstacles to building new border crossings and expanding existing border infrastructure. If the answer is "no" to the second question, the president and Congress may want to reconsider their current position on the first. It may be better to scale back the requirements and expectations of US-VISIT rather than develop a system that cannot accomplish the unrealistic goals set out for it.

The deployment of new screening systems that citizens can see in operation may increase their sense of security. These new systems may also provide examples of what the government is doing to protect its citizens. However, if these new systems are not complete, if they are easily countered or bypassed by the determined terrorist, they may end up providing more of a sense of security to citizens than actually making them more secure. Policymakers are often reluctant to ask their own citizens to sacrifice—to wait longer for proper inspections at borders, to pay more for international travel, to submit biometrics for more secure travel documents. It is much easier to envision a technological solution and promise that it will have little, if any, impact on citizens' lives and pocketbooks. It is not yet clear what US-VISIT will be able to accomplish, but this largely depends on the willingness of Congress and the president to ask the American people to make a few sacrifices.

ADVISORY BOARD

ACKNOWLEDGMENTS

I am very grateful to the Migration Policy Institute for sponsoring the project titled "An Assessment of Selected US Border Control Measures after September 11,"of which this report is a part. Special thanks go to Deborah Meyers for managing the project, organizing the February 17, 2005 project workshop, and providing editorial guidance. I thank the members of the project advisory board and workshop participants who provided very helpful comments and suggestions. I am also very grateful to the Woodrow Wilson Center for International Scholars for supporting my research for this report while I was a fellow of the Center in Washington.

ABOUT THE AUTHOR

Rey Koslowski is Associate Professor of Political Science at Rutgers University – Newark; Faculty Fellow of Rutgers' Center for Global Change and Governance and Director of the CGCG's Research Program on Border Control and Homeland Security. In September 2005 he will move to the University at Albany, State University of New York with a joint appointment in the Political Science Department and the School of Information Science and Policy. Dr. Koslowski has held fellowships at the Woodrow Wilson International Center for Scholars, the Center of International Studies at Princeton University, and the Center for German and European Studies at Georgetown University's School of Foreign Service. He is the author of *Migrants and Citizens: Demographic Change in the European States System* (Cornell University Press, 2000), co-editor (with David Kyle) of *Global Human Smuggling: Comparative Perspectives* (Johns Hopkins University Press, 2001) and editor of *International Migration and the Globalization of Domestic Politics* (Routledge, 2005). His articles have appeared in *International Organization, International Studies Quarterly, The Journal of Common Market Studies, The Journal of European Public Policy, The Journal of Ethnic and Migration Studies, The Cambridge Journal of International Studies,* and *The Brown Journal of World Affairs*. During the coming year, he will be devoted to a research project entitled "International Migration and Border Control in the Information Age: European, Transatlantic and Global Dimensions" and supported by a Research and Writing Grant from the John D. and Catherine T. MacArthur Foundation.

This report is the first in a series of three released by MPI for its project Assessing Selected Border Control Measures After September 11.

The aim of this project is to evaluate the implementation and impact of border-related changes to date, comparing the outcomes against stated goals. In doing so, the authors hope to fill a vacuum in independent research and provide the analytical backbone for policy discussions on issues that need to be addressed as the government presses forward with sweeping changes. The reports highlight areas in need of improvement and make constructive suggestions for mid-course corrections that are critical to the long-term success of the programs and for US security. Other releases in this series include:

One Face at the Border: Behind the Slogan
By Deborah Waller Meyers, Policy Analyst, Migration Policy Institute (June 2005)

Secure Borders, Open Doors: Visa Procedures in a Post-September 11 Era
By Stephen Yale-Loehr, Adjunct Professor of Law, Cornell University; Demetrios G. Papademetriou, President, Migration Policy Institute; and Betsy Cooper, Research Assistant, Migration Policy Institute (Summer 2005)

These reports and other MPI publications are available through MPI's online bookstore at www.migrationpolicy.org.

1400 16th Street NW
Suite 300
Washington, DC 20036

202 266 1940
202 266 1900 fax

www.migrationpolicy.org