International Cooperation to Create Smart Borders

Rey Koslowski

Woodrow Wilson International Center for Scholars and Rutgers University-Newark

Prepared for the conference on *North American Integration: Migration, Trade and Security*, organized by the Institute for Research on Public Policy (IRPP) in collaboration with the John Goodwin Tower Center for Political Studies at Southern Methodist University, Fairmont Chateau Laurier, Ottawa April 1-2, 2004.

Acknowledgements: The research for this paper was supported by a fellowship from the Woodrow Wilson International Center for Scholars.

DRAFT: Comments and suggestions most welcome.

Contact info:
Rey Koslowski
Fellow
Woodrow Wilson International Center for Scholars
1300 Pennsylvania Ave. NW
Washington, DC 20004-3027
Tel: 202-691-4066
email: koslowskirj@wwic.si.edu
http://www.wilsoncenter.org/index.cfm?fuseaction=sf.profile&person_id=34921

After May 30, 2004:
Political Science Department
Rutgers University-Newark
Newark, New Jersey 07102
Tel: 973-353-5048
email: rkoslowski@earthlink.net
http://tecn.rutgers.edu/politicalscience/koslowski.html

Introduction

In the wake of the September 11th attacks on the World Trade Center and the Pentagon the United States rapidly stiffened its border controls. Given the initial perception in the U.S. that the Canadian border was a sieve through which terrorists could easily pass, the U.S. redeployed Border Patrol officers to the U.S.-Canadian border. Inspections were also stepped-up on the southern border with Mexico and U.S.-Mexican negotiations over a temporary worker program and amnesty for Mexicans quickly faded into history. While the initial response to September 11 involved a massive increase of inspections at border crossings with Mexico and Canada, this quickly led to traffic back-ups of 15 hours at the U.S. Canadian border – delays that could not be economically sustained.

In response to these conflicting security and economic imperatives, the U.S. and Canada began talks on exploring the possibility of building a "North American Perimeter" modeled after the European Union, whereby internal border controls are lifted as a common external border is established. These talks shifted focus toward international cooperation that would leverage information technology, yielding an "Action plan for Creating a Secure and Smart Border," announced on December 12, 2001 (White House 2002a). On March 22, 2002, Presidents Bush and Fox announced a similar 22-point agreement to build a "smart border" between the United States and Mexico (White House 2002b). These initiatives to create a "Smart Border" of the future became a central feature of the subsequent National Homeland Security Strategy (White House 2002c). According to a White House statement:

> The border of the future must integrate actions abroad to screen goods and people prior to their arrival in sovereign US territory, and inspections at the border and measures within the United States to ensure compliance with entry and import permits..… Agreements with our neighbors, major trading partners, and private industry will allow extensive pre-screening of low-risk traffic, thereby allowing limited assets to focus attention on high-risk traffic. The use of advanced technology to track the movement of cargo and the entry and exit of individuals is essential to the task of managing the movement of hundreds of millions of individuals, conveyances, and vehicles (White House 2002).

In a dramatic illustration of the Administration's agenda, Richard Falkenrath, 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.[1]

With respect to border control, the U.S. National Homeland Security Strategy is largely based on policy proposals to "push U.S. borders out" (Flynn 2000) beyond U.S. territorial boundaries. U.S. border control authorities have deputized airline agents to inspect the travel documents of U.S.- bound passengers, there has been increasing forward deployment of U.S. Immigration and

[1] Response to author's question at "Transatlantic Homeland Security? European Approaches to "Total Defense," "Societal Security"and their Implications for the U.S." Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies Johns Hopkins University, Feb. 19, 2004.

Customs Enforcement (ICE) as well as Customs and Border Protection (CBP) officers and the information technology to support them, such as electronic submission of passenger and cargo manifests in advance of departure to the U.S. In many ways, the approach of pushing border control activities outside of the US is analogous to the globalization of production that has transplanted factories abroad (Koslowski 2004). Although state responses to the September 11th attacks demonstrate that the world is far from "borderless," as early apostles of globalization contended (Ohmae 1990), the U.S. response is not just one of "rebordering" (Andreas 2002) with the build-up of traditional border controls physically located at the thin line between states. We are seeing the emergence of very wide zones of transnational border control practices that span the globe. Indeed, as expanding e-government and private sector submission of electronic data enables the pre-clearance 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."[2]

In this paper, I argue that smart borders cannot be totally virtual and significant physical infrastructure investments at the border will be necessary in order to enable new technologies to work their magic. Information systems also require data to be effective and there are significant economic, political and privacy issues that have the potential to become major barriers to implementing the smart borders concept. These infrastructure and data barriers have become particularly apparent through analysis of the new entry-exit system, US-VISIT, which was not part of the original Smart Border agreements but is now becoming the largest DHS information technology deployment. Moreover, the smart borders approach is not necessarily complementary with proposals for a "North American Perimeter," even though they are often conflated in the broader context of bilateral and trilateral cooperation among the U.S., Canada and Mexico.

The challenge of border control after Sept. 11, 2001

The U.S. 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' Bureau of Customs and Border Protection (CBP) has the task of intercepting terrorists at over 300 ports of entry and along the 5,525 mile U.S.-Canadian Border and the 1,989 U.S. – Mexican border. In 2002, $1.4 trillion worth of imports. From 1994 to 2001, total U.S./Canadian surface trade increased from $223 billion to $347 billion and U.S. Mexican surface trade increased from $88 billion to $201 billion (DHS 2003). Given that the volume of U.S. international trade doubled during the 1990s, while Customs inspection personnel increased only by 7% during the decade (MITRE 2000), Customs and Border Protection has been trying to screen potentially dangerous cargo and people out of the flows of legitimate trade and travel with only three fifths of the human resources relative to the increased flows.

[2] This is the term used by Commissioner Bonner in remarks at reception preceding the 2003 Customs and Border Protection Trade Symposium, Nov. 19, 2003.

Moreover, the attacks demonstrated the vulnerability of the U.S. economy to shutdowns of the transportation system. The grounding of commercial air traffic and heightened border security after the September 11th attacks amounted to the United States doing to itself what no enemy has done before: an embargo on trade (Flynn 2002). This self-embargo demonstrated the vulnerability of extended supply chains and trans-border just-in-time manufacturing, most dramatically on the U.S.- Canadian border. Up to 10 million vehicles annually cross the Ambassador Bridge between the Windsor, Ontario and Detroit, Michigan, along with 27% of U.S.-Canadian Merchandise trade.[3] Shortly after the attacks, traffic backed up to 15 hours at the U.S.-Canadian border (Audi 2001). Within days of the attacks, Daimler-Chrysler announced that it would have to stop several U.S. assembly lines for want of Canadian parts caught in the traffic back-ups at the border. Ford Followed suit shortly thereafter.

In terms of growing flows of people, 440 million people entered through U.S. ports of entry and were a total of 358,373,548 entries through land ports of entry with Canada and Mexico during fiscal year 2002 (DHS 2003: 1, 16). It has been estimated that there are now 9.6 million undocumented migrants in the U.S. (Passel, Capps, Fix 2004), approximately 40% of whom entered legally but overstayed their visas. The September 11, attacks exposed the security consequences of increasing migration and travel as terrorists used the same modalities of visa abuse and identity document fraud characteristic of illegal migration to the U.S. At least 2 of the highjackers used fraudulent passports (9-11 Commission 2004), one with a student visa never showed up for class, three had stayed in the U.S. after their visas expired and several purchased fraudulent New Jersey driver's licensees and Virginia ID's on the black market that primarily services illegal migrants.

Moreover, it became clear that if terrorists could take clandestine routes that transnational criminal organizations use to smuggle illegal migrants into the U.S. For example, a month after the Sept. 11th attacks, Italian authorities found Amir Farid Rizk, an Egyptian-born Canadian national inside a shipping container bound for Canada along with a global satellite phone, laptop computer, airport maps, airport security passes and an airplane mechanic's certificate. Italian authorities suspected that he was an Al Qaeda operative and arrested him under Italy's new anti-terrorism law but then released him several weeks later (Toronto Star 2001). The case demonstrated how easy it might be for a terrorist to enter the U.S. in the same way that migrants have been smuggled in shipping containers.

Before September 11th there was much talk of a borderless world with integrating economies of seamless extended supply chains that enabled globally organized production based on lean inventories and just-in-time manufacturing techniques. Many firms began to treat customs and immigration controls at international borders as a bit of friction in the gears of accelerating international trade and globally organized production. During the 1990s, the U.S. Customs Service and the Immigration and Naturalization Service attempted to accommodate the private sector's need for more efficient processing of paperwork necessary to facilitate international trade and travel but these agencies were limited by miserly information technology budgets and stymied by the political conflict between the U.S. government and the private sector over who would pay for systems that would speed processing at the border. After September 11th, the era

[3] See http://www.ambassadorbridge.com/facts.html

of benign globalization and trade facilitation on the cheap came to an end and the era of ensuring transportation and border security supported by growing information technology budgets began.

Border Security Initiatives Towards "Smart Borders"

The U.S.-Canadian Smart Borders plan includes using biometric identifiers for permanent resident cards and travel documents, sharing advance passenger information from the U.S. Advanced Passenger Information System (APIS) system and its Canadian counterpart, developing compatible immigration databases, such as Canada's Support System of Intelligence, expanding the NEXUS pre-approved passenger vehicle program as well as the NEXUS air pilot program (White House 2002a). Frequent travelers who enroll in the NEXUS program submit information for criminal and terrorist background checks. An enrollee then receives a radio frequency identification (RFID) proximity card. The RFID tag on this card is read at the port of entry and 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 system on the US-Mexican border is similar but it uses a transponder attached to the commuter's vehicle rather than a proximity card held by an individual. The US-Mexican Smart Borders plan would expand dedicated SENTRI commuter lanes at high-volume ports of entry along the U.S.-Mexico border, set up advance passenger information exchanges for flights between Mexico and U.S. and develop systems for exchanging information and sharing intelligence (White House 2002b).

Both plans are premised on bilateral cooperation that enables the U.S. to deploy information technology in order to practice risk management targeting of vehicles, shipments and travelers and to push its "borders out" while at the same time attempting to minimized the impact of border controls on trade and travel. By the Spring 2003, significant strides were made in realizing many of the specific objectives in the U.S.-Canadian agreement; having fewer specific action points to begin with in the U.S.-Mexican agreement, progress was made in certain areas of cooperation, particularly those that did not require major increases in funding (Myers 2003). Further progress on the U.S.-Canadian Smart Border agreement was announced on Oct. 3, 2003, highlighted by completed NEXUS implementations at nine ports of entry and six more scheduled to be completed by the end of 2003 (U.S. and Canada 2003).

These Smart Border Agreements are complementary, if not integral, to several major U.S. border security initiatives. In January of 2002 U.S. Customs Commissioner Bonner announced the Container Security Initiative (CSI) that pre-screens cargo containers at ports of origin or transit rather than when they reach the U.S. (Bonner 2002). Canada was the first country to cooperate with the U.S. on container security and in a sense this cooperation served as a pilot for the broader CSI program. CSI agreements are reciprocal. U.S. Customs inspectors have been deployed in Halifax, Vancouver and Montreal, Canadian inspectors in Newark and Seattle.

In April 2002, Commissioner Bonner announced the creation of the Customs-Trade Partnership Against Terrorism (C-TPAT), a public-private partnership to increase the security of cargo while facilitating trade. As Commissioner Bonner put it, "The message should be clear-if a business takes steps to secure its cargo against terrorism, we will give it the 'fast lane' through the border

(U.S. Customs 2002)." Seven companies helped to establish the program - BP America, Daimler Chrysler, Ford Motor Company, General Motors Corporation, Motorola Inc., Sara Lee Corporation, and Target (U.S. Customs 2002). It is not an accident that the big three automakers figure prominently among the founders. Over 4,000 companies have signed agreements. The popularity of the program reflects the fact that in context global competition, "fast lane" is the only lane.

In a certain sense, the forward deployment of U.S. Customs personnel with the Container Security Initiative draws on model of longstanding cooperation between the U.S. and Canada on immigration. U.S. immigration inspectors have long operated beyond U.S. borders – in Canada. Ever since an agreement signed in 1894, U.S. inspectors posted at Canadian ports of entry have inspected U.S.-bound immigrants. Immigration inspectors were subsequently posted to Canadian airports to conduct "pre-inspections," that essentially cleared U.S.-bound passengers through U.S. passport controls of flights from abroad connecting through Canadian airports. Fly into the US from Japan via Vancouver or Toronto and you will be greeted by U.S. Customs and Border Protection inspector.

Point 8 of the U.S.-Canadian Smart Border Agreement outlines an agenda for cooperation on advanced passenger data and point 17 deals with customs data. The Aviation and Transportation Security Act passed by the US Congress in the Fall of 2001 requires that airlines with US-bound international flights electronically submit a passenger manifest with data including full name of each passenger, date of birth, sex, passport number and country of issuance, US visa number or alien card number.[4] The subsequent 2002 US Enhanced Border Security and Visa Entry Reform Act requires commercial airlines and ships to electronically submit passenger and crew manifests before arrival to the US via the Advanced Passenger Information System (APIS), sets out fines for non-compliance and loss of landing rights for those airlines that have not paid their fines.[5] Canada also deployed its passenger information system (PAXIS) at Canadian airports in October 2002 and began collecting passenger name record (PNR) data (Auditor General 2004). Canada and the U.S. have agreed to share passenger manifests and passenger name records using an automated data-sharing and program that will also assess risks of the passengers in question. This system is scheduled to be in place by Spring 2004 (U.S. and Canada 2003).

In order for the vision of the Container Security Initiative of pre-screening of containers in the port of origin to work, CBP needs information about the contents of containers in order to determine whether or not they should be x-rayed and/or physically inspected. On Dec 2, 2002, U.S. Customs instituted a new regulation that requires by advanced electronic submission of cargo manifests 24 hours before U.S. bound sea containers are loaded (Bonner 2002a). Electronic manifest information must be submitted two hour before arrival for rail shipments into the U.S. and one hour prior to arrival for trucks unless in the Free and Secure Trade (FAST) program which can submit data up to 30 minutes before arrival.[6] In response to these advanced electronic data submission requirements, David Bradley, President of the Canadian Trucking Alliance expressed concern about these requirements and noted that "if just-in-time becomes

[4] Section 115 of the ''Aviation and Transportation Security Act,'' Public Law 107–71, Nov. 19, 2001

[5] Section 402 of the ''Enhanced Border Security and Visa Entry Reform Act of 2002,' Public Law 107–173, May 14, 2002.

[6] Section 343, Trade Act of 2002.

problematic, industry will just ship production to the U.S." (Quoted in Halifax Daily News 2003). Despite such concerns, companies have managed to meet advanced data submission requirements. In the future, customs authorities could tap private sector logistics systems to such an extent that border controls may begin at the point a shipping notice is entered in manufacturers' inventory, warehousing and distribution systems.

Entry-Exist Systems: US-VISIT

In response to the Sept. 11th attacks, the U.S. Congress passed new border security legislation that mandated the implementation of an entry-exit system, which was re-launched as United States Visitor and Immigrant Status Indicator Technology (US-VISIT). This was not the first entry-exit system proposed by Congress. Section 110 of the U.S. Illegal Immigration Reform and Immigrant Responsibility Act of 1996 mandated that 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"[7] and to do so by the end of 1998. Congress pushed back the deadline for implementation of the law in October 1998 after lobbying by U.S. business groups from states bordering Canada (Cohn 1999: 25-38). These groups pointed out that registering every person who crosses into the U.S. from Canada using even smart card technology would still require enough processing time to back up traffic at the border for hours, especially at the Detroit – Windsor crossing. This was a particular sore point for the big three automakers given that their just-in-time production lines crossed the border. 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; the 50 most highly trafficked land ports of entry by the end of 2004 and all ports of entry by the end of 2005. In practical terms, however, the DMIA put an indefinite hold on deployment 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 and barred the INS from requiring additional entry-exit data.[8]

The visa tracking system that existed prior to Sept. 11, 2001 primarily covered passengers arriving by airplane and consisted of a paper form stamped at the port of entry, which is supposed to be returned to the airline upon departure and then entered manually into the database of the legacy INS non-Immigrant Information System (NIIS). Due to lost forms, incomplete data entry, entry and 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 have overstayed their visas – as was the case of several of the September 11th 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 office noticed

[7] Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Section 110.a.1 Automated Entry-Exit Control System," U.S. Congressional Record – House, September 28, 1996, p. H11787.
[8] See "Data Management Improvement Act of 2000," Public Law 106-215.

that he had overstayed his visa by over a month on his previous trip to the U.S. A former INS officer, Patrick Pizarro, explained that the inspectors most likely missed Atta's overstay because they are under pressure allow to clear tourists as quickly as possible but "'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.'" (quoted in Chardy 2001). After September 11th, incoming passengers received greater scrutiny but, according to an INS inspector from Miami who appeared on CBS' "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 look out databases (CBS 2002).

In response to these failures, Congress passed and President Bush signed the Enhanced Border Security and Visa Entry Reform Act in 2002.[9] The law reiterated the DMIA mandate and timetable for implementation of an entry-exit system. The Bush Administration's 2003 budget allocated $380 million for the implementation of this comprehensive entry-exist information system (Ziglar 2002). The US-VISIT program budget was $328 billion in FY 2004 and $340 million in FY 2005 adding up to well over $1 billion through the end of 2005 (DHS 2004: 17). The DHS estimated that overall cost of the system would be $7.2 billion through FY 2014 but the GAO calculated that its 10-year cost could be as much as twice that (Hite 2004).

According the November 2003 Request of Proposals, US-VISIT is envisioned as a comprehensive border management system enabling "end-to-end management of processes and data on foreign nationals to the United States covering their interactions with U.S. officials before they enter, when they enter, while they are in the U.S. and when they exit" (DHS 2003a: 8). A prime contractor and its team of companies will develop this comprehensive system but the prime contactor is not scheduled to be selected until May 2003. In the meantime, DHS scrambled to meet the Congressional deadlines by rolling out increment one of US-VISIT which is basically a collection of interfaced legacy systems including the Arrival Departure System (ADIS), Advanced Passenger Information System (APIS), Interagency Border Inspection System (IBIS), Automatic Biometric Identification System (IDENT), Student Exchange Visitor Information System (SEVIS), Computer Linked Application Information Management System (CLAIMS 3) and the Consular Consolidated Database (CCD) (Hite 2004: 8). This first version of US-VISIT went live January 5, 2004 when DHS began to collect digital photographs and fingerprint scan biometrics from those individuals traveling on a non-immigrant visa to the United States upon entry at 115 airports and 14 seaports. After biometrics and passport data are collected watch list checks are run on the data while inspectors ask routine questions regarding reasons for visiting, etc. US-VISIT adds an average of 15 seconds to the entry process and as of March 17, 2003, 2 million people were processed through US-VISIT entry procedures (Mocny 2004).

In order to address the loopholes that allowed some members of al Qaeda to enter on U.S. visas, Congress mandated that all US visas incorporate a biometric identifier by October 26, 2004 and a combination of facial recognition and electronic fingerprint scanning was selected as "the most effective and least intrusive (Jacobs 2003)." A digital photograph and fingerprint scans will be taken of all non-immigrant visa applicants at US embassies and consulates and then these

[9] ''Enhanced Border Security and Visa Entry Reform Act of 2002,' Public Law 107–173, May 14, 2002.

biometrics will be compared with biometrics collected upon arrival at the port of entry through the US-VISIT program.

Initially, the requirement for biometric enrollment in US-VISIT upon entry did not apply to nationals of the 27 states in the U.S. Visa Waiver Program who are permitted entry into United States without a visa for a stay of up to 90 days. The Enhanced Border Security and Visa Entry Reform Act, however, conditions countries' participation on the issuance of machine-readable, tamper-resistant passports containing biometric data and sets a deadline of Oct 26, 2004. Given that many countries could not meet this deadline, it would be very difficult for the Sate Department to process their visa applications in U.S. consulates and the impact on tourism and travel could be very costly to the U.S. economy, Secretaries Tom Ridge and Colin Powell have asked Congress for a postponement to December 2006 (Powell and Ridge 2004). Shortly thereafter, DHS announced that nationals of the 27 Visa-Waiver counties will be required to enroll in US-VISIT and submit to a digital photograph and finger scanning upon entry beginning September 30, 2004 (Stout 2004).

Beginning in October 2004, Canada will be the only country whose nationals may enter the U.S. without submitting biometrics. This will make Canadian passports increasingly valuable on the black market serving human smugglers. This is particularly the case for passports issued before new passports with digitized embedded photos began to be issued starting May 2002 and fully deployed by the end of 2003. Older passports valid for up to five years from date of issuance have laminated photos that are more easily altered by photo substitution and used by another person. Increased demand for stolen Canadian passports may not only present an increasing problem for Canadians traveling abroad; the Royal Canadian Mounted Police are concerned that criminals and terrorists may use these passports. European police have found evidence that a group linked to the Madrid bombing, Ansar al-Islam, has been running a human smuggling and document fraud operation to fund terrorist actions as well as to smuggle its own members into countries like Spain and Iraq (Simpson, Crawford and Johnson 2004). There are already 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, due to privacy considerations, the Passport Office does not share its list of deactivated passports with Citizenship and Immigration Canada and inspectors at Canadian ports of entry cannot identify deactivated passports (Auditor General 2004: 31-32). As of February 2004, data on lost and stolen passports has been manually entered into RCMP databases (Passport Office 2004) but the Auditor General report noted high error rates and data entry lags (Auditor General 2004: 31). If data on lost and stolen Canadian passports are not also shared with U.S. authorities, Canadian passports stolen in Canada or abroad could be photo substituted and used by individuals to enter the U.S. without submitting biometrics and being subject to criminal and terrorist biometric watch lists.

The US Congress deferred to the International Civil Aviation Organization (ICAO) on setting the biometric standard for the required biometrics in passports issued by Visa Waiver countries and it was not until May 28, 2003 that the ICAO announced an agreement - facial recognition plus optional fingerprints and/or retina scans which are stored on contactless integrated circuit (IC) chips (ICAO 2003). The contectless IC chip and other Radio Frequency Identification (RFID) technologies are central to the vision of the “revolution in border security.” The contactless IC chip is part of an RFID 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. As opposed to machine-readable travel documents that contain data on magnetic strips, a passport with a contactless chip can be read by the reader at a distance, therefore allowing faster transfer of data from the passport. Similar applications include Washington, DC Metro Smartrip cards, which are read by touching a pad on turnstiles triggering deduction of the fare from the digital account on the embedded chip.[10] As envisioned, holders of new biometric passports issued by Visa Waiver countries will give their passports to CBP inspectors who will simply bring the passport close to the reader. The reader will capture the personal data and the digitized biometric. 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 into the US. Similarly, upon exiting within the 90-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.

Infrastructure and Data

The fundamental problem of the previously partially deployed entry-exist system still exists. A tracking system cannot determine who is in the country if the data are not complete. For example, a record of an entry may be entered in the database when someone enters by air, but if that person departs at a land border, a corresponding exit record is not registered. When asked, at a Fall 2003 meeting, DHS staff in charge of inspections referred to land border exits and the capture exit data as a "work in progress" with no plans yet for staffing.[11] As late as 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 (Mocny 2004)." Apparently, the exit plan will not be articulated until after the prime contractor and the team of companies that will develop US-VISIT is selected in May 2004.

If data is not collected on every entry and corresponding exit, the database will not be complete and subject to persistent errors. After the US-VISIT program had been established, it was announced that, for the time being, Canadian nationals would be exempt from mandatory enrollment in US-VISIT (Canadian Embassy 2003). In response to Mexican objections of unequal treatment in comparison with the U.S.'s other NAFTA partner, the Bush administration has decided to exempt Mexican nationals with border crossing cards (so-called laser visas) that entitle holders to enter the U.S. and remain in the border region up to 25 miles into U.S. territory for up to 72 hours (Pfister 2004; DHS n.d.). The Border Trade Alliance, a business group representing over 1,000 industry, government and education officials said the plan does not go far enough and hopes that border crossing cards could be valid for stays of 6 months and good for travel throughout the Southwest (Cantlupe 2004).

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

[10] See http://www.wmata.com/riding/smartrip.cfm

[11] Response to author's question at Customs and Border Protection's Trade Symposium, Nov. 2003.

and biometric data of the Mexican nationals with Border Crossing Cards as well as data collected from those Canadians enrolled in the NEXUS program.[12] Even if interfaces are built between these legacy systems, the absence of pre-existing data standards may preclude adequate data sharing between US-VISIT, the Border Crossing Card databases and NEXUS databases (See DHS 2003: 124-137, DHS 2003b: 22-26). 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 in the Border Crossing Card and NEXUS programs, and even if this involves more data than collected by US-VISIT, data from Border Crossing Card and NEXUS databases are not necessarily useable for an entry-exit system.

While the exemptions of Canadian and Mexican nationals from US-VISIT enrollment are completely understandable from an economic and political perspective, if records generated by the entries and exits of 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. Records of items may be generated through data entry at the loading dock or with barcode scans and, in the near future, with RFID systems. If you want an accurate report about 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 needs 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 will be inaccurate, even if most of those items eventually leave 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 US, unless all of their data is entered into the system.

The problem of physical infrastructure also remains. As Geronimo Gutierrez, the Under-Secretary for North America at the Mexican Secretariat of External Relations, put it, "We have pre-NAFTA infrastructure at our borders" (Gutierrez 2004). With new data collection requirements on top of increasing trade and travel flows, it may become be impossible to process visitors and shipments without backing up traffic unless larger secure areas at border crossing are cleared for inspection lanes and booths and unless more bridges and tunnels are built, especially

[12] Author's discussion with DHS official, April 9, 2004.

between the Canada and the U.S. Even with without the new requirements of US-VISIT, many land ports of entry do not have sufficient space for current operations, indeed 64 ports of entry have less than 25 percent of the space they require (DHS 2003).

Exit controls for US-VISIT at land borders would mirror entry controls with the construction of additional lanes and booths, the installation of biometric readers and workstations and the hiring inspectors to process the exits. As far as the additional costs of 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 but this figure assumes that no additional lanes would be required for entry and exit lane requirements would be the same as those for entry (Hite 2004).

Exit controls at land borders that did not include a primary inspection by a DHS officer might save billions of dollars but it may be next to impossible for US-VISIT to achieve its objectives of determining whether someone has overstayed or should be apprehended when leaving. While the ICAO and US-VISIT program have great hopes for using RFID technology to expedite travelers through border controls at ports of entry, there are limits to what can be securely automated at the border controls of “ports of exit.” An RF-based exit system may record the exit of a travel document with biometrics on a RFID chip (or the RFID chip) 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 biometric on the chip.

According to the US-VISIT Request for Proposals (RFP) “As foreign national travelers leave the U.S., 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.” (DHS 2003a: 9). 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.” (p. 118) and “The Contractor’s exit solution cannot assume that vehicles can be stopped in traffic lanes” (p.121).

It is hard to envision how an RFID system would automatically “check out” biometric visa or passport holders as they drive through exit lanes and be able to determine whether the person leaving a visa 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 U.S. visa or ICAO compliant biometric passport and exit the U.S. as a passenger of a car driven through the exit lane into Canada. The travel documents could then be sent back to the criminal or terrorist remaining in the U.S. while US-VISIT has a record of him departing into Canada.

Even if the RF system did register a “hit,” what could U.S. authorities do if the suspect has already crossed the border into Mexico or Canada, especially if the individual in question holds a Mexican or Canadian passport? Are the enforcement measures possible in this situation close to what could be attained with an exit inspection process that was similar to that upon entering (i.e. presentation of travel documents, identity check based on facial recognition and fingerprint scan as well as watch list check)?

These questions point toward intensified international law enforcement cooperation that could potentially solve some of the infrastructure, staffing and data collection problems as well. Instead of building exit booths and staffing them with DHS officers to conduct primary exit inspections, Canadian and Mexican border control officers could simultaneously conduct their entry inspections together with U.S. exit inspections whereby they would collect biographical and biometric data and enter that exit data into US-VISIT. Canada and the U.S. have already shared in infrastructure development at two ports of entry (Oroville, Washington and Sweetgrass, Montana) and there have been discussions of such a shared solution. Such cooperation, however, would require significant cost sharing and a high level of mutual trust. Nevertheless, it may be the best, if not 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 U.S. 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 (see, e.g., Flynn 2003). Such trilateral solutions, however, would require even deeper cooperation.

Bi-lateral and multilateral deployments of information technology to make borders smarter may seem very futuristic but the technology necessary for the mass surveillance and e-government capabilities that might make it possible are increasingly available. As the linking of enterprise systems through the internet has led to a rapid growth of business-to-business e-commerce, public sector versions of these software packages have been developed that could enable governments to mine information from data warehouses and automate exchanges with other governments that do likewise. Within the next decade, the technical capabilities for states to gather and to exchange and mine mountains of data regarding the identity of their citizens and the activities of suspects will be available. Will governments wish to use these capabilities? And if democratic governments opt to use these new capabilities, will the people who elected them allow it?

For example, there are growing privacy concerns that spawn political tensions over biometric submission requirements imposed by the U.S. Photographs can be considered biometrics that can be scanned by facial recognition systems. Requiring passports to contain biometric information beyond photographs, such as fingerprints, retinal scans, hand geometry, etc. is politically and diplomatically problematic. As I explain elsewhere (Koslowski 2004a), there has, nevertheless, been a great deal of cooperation between the U.S. and the EU on transfers of passenger manifests and coordination of biometric standards. Given that Canada and Australia have also passed laws requiring advanced passenger information, the EU is moving the discussion to the global forum of the International Civil Aviation Organization.

While biometric national identity systems and automated transnational information exchanges between law enforcement agencies may be technically possible quite soon, it is unlikely that the transformed information technology environment would be global in scope. The digital divide between developed and less developed states may short-circuit information sharing among governments in migrant receiving, transit and sending states. Therefore, effective international law enforcement information sharing initiatives may only be possible with major financial and technical assistance to law enforcement agencies of less developed countries. For example, while Canadian and U.S. Governments may soon have the IT capabilities to put in place for some of the Smart Border initiatives that they have envisioned, it is not that clear that the Mexican government will be able to deploy the technology needed, nor be able to assure U.S. and Canadian partners that Mexican databases and systems are secure enough for U.S. and Canadian law enforcement officials to share sensitive information. The U.S.-Mexican Smart Border initiative will provide a good test of international border control information sharing as well as the will of rich partners to provide the financial and technical assistance needed to make it work.

Smart Borders vs. North American Security Perimeter

Although the idea of a North American perimeter had been discussed long before Sept. 11, 2001, reactions to the attacks and to the clampdown by the U.S. at the border quickly raised the profile of the discussion. A week after the attacks, U.S. Ambassador to Canada Paul Cellucci said in response to a question, “I think that if we had policies on immigration and refugee status that were more common we could establish this perimeter to protect the United States and Canada, and I think that is where we should be headed (Cellucci 2001).” Canadian business groups were quick to endorse the approach. Perrin Beatty, President and CEO of the Canadian Manufacturers and Exporters (CME) argued, “A perimeter approach to security would ensure the protection of both Canada and the United States from external threats while allowing relatively free movement between the two countries” and 88% of the respondents to a questionnaire distributed at the CME convention also favored a North American perimeter. (Canadian Newswire 2001). Members of the Canadian government, however, were not that interested in adopting harmonized security and immigration policies with Foreign Affairs Minister John Manley saying “the notion that we can somehow or another solve a perceived problem by something called a perimeter is just rather simplistic to me” (quoted in Fraser 2001). After announcing that Canada and the U.S. were discussing moves to reduce the difference between the two in the list of countries whose nationals are required to have a visa for entry, former Immigration Minister Elinor Caplan remarked, “When you say “perimeter,” people think the European model where you erase the internal borders. That is not what we are talking about” (quoted in Alberts 2001).

In response to the reluctance of the Canadian Government, Fred McMahon, Director of the Centre for Globalization Studies at The Fraser Institute, argued, “ Imagine the boost to Canadian businesses if goods could move across the Canada-US border as quickly as they can the German-French border. Imagine the convenience for individual Canadians crossing the border…The European model would require some coordination of Canadian immigration policy with that of the United States, something European nations have already put in place. This hardly means that immigration policies must be identical in the US and Canada and Mexico any more than they are identical in Europe (McMahon 2001).” In comments at a meeting to commemorate the 10th anniversary of NAFTA, Former Prime Minister Brian Mulroney also weighed into the debate in favor of a security perimeter, saying, “The NAFTA partners must dedicate themselves as a matter of the greatest urgency to building an area of security in North America, one that denies terrorism a foothold on our continent and insures uninterrupted legitimate flows among us. Such common action is also essential to allow us to protect the great North/South flows of goods, people, technology that underpins our shared prosperity. Our internal borders will only be smart if our external perimeter is secure" (Mulroney 2002). Mr. Mulroney's speech propelled the notion that efforts to modernize borders between the U.S. and Canada through the deployment of new technology must be complemented by building a North American perimeter through the harmonization of policies. In the rest of this section, I will critically examine European model for North American border control and consider the extent to which smart borders are complementary to a North American perimeter.

During the 1980s, intra-European trade and intra-European travel increased while at the same time shipments increasingly went by truck and more Europeans drove cars. This became a recipe for huge backups at borders as trucks and tourists stopped at borders for passport inspections. A trans-European shipment could easily involve crossing two or three borders with waits totaling longer than the time on the road between borders. Since the European Community (EC) member states had entered into a customs union in 1968, the cargo that trucks carried was not subject to duty payments when crossing internal borders. To address this problem, Germany, France, Belgium, the Netherlands and Luxembourg signed an agreement in 1985 to gradually abolish internal border checks, in the small Luxembourg border town of Schengen. Shortly thereafter the members of the European Community signed the 1986 Single European Act (SEA), which set out a course for realizing the free movement of goods by eliminating non-tariff barriers to trade, establishing free movement in services and persons and do so by 1992. The rights of nationals of one EC member state to work in another does not mean unimpeded travel across borders, however, given the growing lines at the border, there was increasing pressure for EC member states to lift border controls between states. Therefore a subset of EC member states built on the 1985 Schengen Agreement by signing Schengen Convention in 1990. The Schengen Convention therefore harmonizes asylum application procedures and mandates that asylum seekers may only apply in one country. It also calls for a common visa policy, harmonization of polices to deter illegal migration and an integrated automated information system so as to coordinate actions regarding individuals who have been denied entry. All customs controls at internal borders within the newly established European Union were lifted in 1993 and Schengen Convention went into effect in 1995 lifting internal border controls while establishing a common external border. Mr. McMahon is correct, in order for the U.S., Canada and Mexico to adopt the European model, immigration policies would not have to be identical, however, the European model presupposes a customs union and requires identical visa policies.

There are some difficult political questions for those who argue for lifting internal border controls within a North American perimeter, beginning with the question of Cuba. Would the U.S., Canada and Mexico be able to come to agreement the same set of tariffs on goods imported from Cuba? As to the Canadian and Mexican cases, I will leave this question to those more knowledgeable of Canadian and Mexican domestic politics. The prospect of President Bush proposing to lift the embargo on Cuba for the sake of harmonizing tariffs with Canada and Mexico policies is rather dim given that the support of those Cuban Americans who oppose lifting the embargo is essential to a Republican victory in Presidential primaries in the swing state of Florida. Even if President Bush were to expend the political capital to propose lifting the embargo, it is questionable as to whether or not a sufficient number of Republicans in Congress would support him, as it is increasingly becoming clear with respect to his proposal on immigration reform. While the election of a Democratic president may change the political dynamics, John Kerry elected president it is far from certain that he would call for lifting the embargo, especially after the current campaign. Although Kerry was quoted in a 2000 interview calling a reevaluation of the trade embargo "way overdue," in a recent radio interview he stated, "I'm pretty tough on Castro, because I think he's running one of the last vestiges of a Stalinist secret police government in the world…and I voted for the Helms-Burton legislation to be tough on companies that deal with him." (quoted in Wallsten 2004). So, if it is unlikely that the U.S. would drop it's trade embargo on Cuba in the near future, would Canada and Mexico be willing to join in the embargo for the sake of lifting internal border controls with the U.S.?

There are similar challenges for developing a common visa policy. In order to enter the United States, nationals of all but 27 states must apply for and receive a visa. The Visa Waiver Program has specific requirements of states as discussed above and states may be added or dropped from the program. Canada and Mexico have similar policies exempting nationals of some states from the requirement to have a visa for entry. The U.S., Canadian and Mexican exemption lists do not, however, coincide. For example, nationals of South Korea, Botswana, Mexico and residents of Hong Kong and a host of British dependencies and Commonwealth countries do not need a visa to enter Canada but these countries are not in the U.S. Visa Waiver Program. Similarly, nationals from many Latin American countries do not need visas to enter Mexico but do to enter the United States. Given that visa-free travel to Canada and Mexico not only reflects strong historical ties but also corresponds to major tourist flows and business relationships, how realistic would it be for Canada and Mexico to cut their visa exemption list to that of the United States? Given that after Sept 11, 2001, members of Congress had entertained the idea of eliminating the Visa Waiver Program all together, it is unlikely that major expansion of the Visa Waiver list to encompass Canadian and Mexican lists are feasible in the near future. Moreover, even if Congressional support emerges for adding particular countries to the Visa Waiver Program, such as the recent introduction of Congressional resolution in support of Poland's petition for visa-free travel, these countries might not coincide with Canadian and/or Mexican lists –thereby widening rather than narrowing the discrepancies among the visa exemption lists of all three countries. Even if the U.S. were to expand its visa waiver list as Canada and Mexico contracted theirs, those countries added would have to meet biometric passport requirements that EU member states will have difficulty meeting in the near future. In light current political dynamics, would it be politically feasible for Mexico to require visas of all Latin American countries? Would it be political feasible for Canada to require visas of fellow members of the British Commonwealth or the rich Hong Kong Chinese investors that Canada so successfully recruited to immigrate to Canada in the 1990s?

Without even moving onto the issues of harmonizing asylum policies and establishing an integrated information system, the political barriers to a customs union or common visa policy between the U.S. and Canada (let alone all three NAFTA partners) will be difficult to surmount. It is possible that leaders of the U.S., Canada, and Mexico may some day overcome these obstacles but unlikely within the timeframe of the border security legislation passed by the U.S. Congress.

Conclusion

Smart borders are not just a matter of deploying hardware and software; they require international cooperation and lots of it. Existing smart border agreements lay out an agenda for extensive international cooperation but even more cooperation will be necessary to collect the necessary data for the smart border concept to work in practice. The "revolution in border security" that moves from smart borders to virtual borders, ironically, requires significant physical infrastructure investments at or near the border in order to work as envisioned. International cooperation can also reduce the overall costs of necessary infrastructure, however, international cooperation in joint border infrastructure development and joint inspections may be too controversial politically in the immediate future. The upshot: significant economic and political barriers to implementing the smart borders concept remain outstanding.

An alternative to making borders smarter is to get rid of borders altogether within a North American perimeter (whether among all three NAFTA members or just between the U.S. and Canada). If policymakers are convinced that lifting internal borders by establishing a North American perimeter is the best way to proceed, it makes little sense to invest billions of dollars in acquiring land and building infrastructure at the border only to have cars and trucks speed through abandoned facilities after border controls are lifted. If a customs union, harmonized visa policy and harmonized asylum policy are judged to be politically feasible in the next few years, then those policymakers who believe in the North American perimeter idea should press forward and begin harmonizing policies immediately before billions are wasted on border infrastructure.

If a North American perimeter is not realistic politically, yet it is still held out as an alternative to building physical infrastructure, the hope for a North American perimeter could reduce political support for the increases in budgets, taxes and fees necessary to realize the "smart borders" vision in practice. Rather than taking an either/or position, one could advocate moving forward with the smart borders initiatives while at the same time reducing discrepancies in customs duties, harmonizing visa and asylum policies as well as building up border control capabilities at external border of the North American community (see, e.g., Dobson 2002: 30, Hufbauer and Vega-Canovas 2003). This is a very reasonable strategy but political capital is not infinite. Political leaders must pick and choose their battles.

If business groups support politicians who tell them what they want to hear about borders disappearing behind a North American perimeter and withhold their support for politicians who call for raising taxes and fees to build more bridges, exit lanes and exit booths at the border, as well as hiring more inspectors to staff them, it is unlikely that border controls meeting the security requirements set by the U.S. Congress will come into being. If voters withdraw support from politicians who call on all Canadians and Mexicans to enroll in US-VISIT and who call on US citizens to accept passports with fingerprint biometrics, it is unlikely that border controls meeting the security requirements set by the U.S. Congress will come into being. If politicians will not expend the necessary political capital and business leaders and citizenries do not support them, it is more likely that a core part of the "smart borders" approach, US-VISIT, will follow in the path of the entry-exit system mandated by 1996 legislation -- partial deployment that ultimately cannot effectively achieve its objectives.

References:

9-11 Commission 2004. “Entry of the 9/11 Highjackers into the United States,” Staff Statement, *National Commission on the Terrorist Attacks Upon the United States*, Seventh Public Hearing, Jan. 26-27, 2004.

Alberts, Sheldon 2001. “Border Deal Would Screen Travelers Before they Arrive,” *National Post*, Nov. 9, 2001.

Andreas, Peter, 2002. “Re-Bordering of America After 11 September,” *Brown Journal of World Affairs* 8:2 (Winter 2002).

Audi, Tamara 2001. “Along the border: Some wait 15 hours to get into U.S.: Entering Canada is easy, but leaving takes motorists a long time,” *Detroit Free Press*, September 14, 2001.

Auditor General 2004. “National Security in Canada-the 2001 Anti-Terrorism Initiative,” Chapter 3 of the *2004 Report of the Auditor General of Canada to the House of Commons*. Downloaded March 30, 2004 at: http://www.oag-bvg.gc.ca/domino/reports.nsf/html/04menu_e.html

Bonner, Robert C., 2002. “U.S. Customs Commissioner Robert C. Bonner Speech Before the Center for Strategic and International Studies (CSIS),” Washington, D.C. January 17, 2002.

Bonner 2002a “Remarks of U.S. Customs Commissioner Robert C. Bonner,”
Trade Support Network, October 9, 2002.
http://www.customs.gov/about/speeches/speech101002.htm

Browning, Douglas M. 2002. Statement at hearing on “Combating Terrorism: Improving the Federal Response,” House Committee on Government Reform, Subcommittee on National Security, Veterans Affairs and International Relations, June 11, 2002.

Canadian Embassy 2003. “Governor Ridge and Deputy Prime Minster Manley Issue One-Year Status Report on the Smart Border Action Plan,” Press Release, Canadian Embassy Washington, DC, Oct. 3, 2003.

Canadian Newswire 2001. “Canada-U.S. Border Concerns Prompt Support for Perimeter Approach to North American Security,” Canadian Newswire, October 2, 2001.

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

CBS 2002. “INS Vigilance Under Fire,” 60 Minutes, CBS News, March 10, 2002. downloaded April 20, 2002 at: http://www.cbsnews.com/stories/2002/03/07/60minutes/main503210.shtml

Cellucci, Paul 2001. Remarks by Ambassador Paul Cellucci at the Canadian Club of Ottawa, September 18, 2001. Downloaded Mar. 20, 2004 at:

http://www.usembassycanada.gov/content/content.asp?section=embconsul&document=cellucci_0918

Chardy, Alfonso 2001. "Atta faced questions about visa at MIA, Flying-lesson plans arouse," *The Miami Herald*, October 19, 2001

Cohn, Theodore H. 1999. "Cross-Border Travel in North America: The Challenge of U.S. Section 110 Legislation," *Canadian American Public Policy* No. 40, Oct. 1999, Occasion paper Series of the Canadian-American Center, University of Maine at Orono.

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

DHS 2003a. "Request for Proposals for US-VISIT Program Prime Contractor Acquisition," RFP No. HSSCHQ-04-R-0096, US-VISIT Office, Department of Homeland Security, Nov. 28, 2003.

DHS 2003b. "Final As-Is Enterprise Architecture Description," U.S. Department of Homeland Security, July, 16, 2003.

DHS 2004. "Budget in Brief, Fiscal Year 2005," Department of Homeland Security.

DHS n.d. "US-VISIT Fact Sheet: U.S. Land Borders" Downloaded Mar 28, 2004 at: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0371.xml

Dobson, Wendy 2002. "Shaping the Future of the North American Economic Space: A Framework for Action," *Commentary*, C.D. Howe Institute, No. 162, April 2002.

Flynn, Steven E. 2000. "Beyond Border Control," *Foreign Affairs*, Vol. 79 no. 6 (Nov./Dec.), pp. 57-68.

Flynn, Stephen, E. 2002. "America the Vulnerable," *Foreign Affairs*, Vol. 81, No. 1 (Jan./Feb.) pp. 60-74.

Flynn, Stephen E. 2003. "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).

Fraser 2001 "Border 'not a problem,' Manley says," *Toronto Star*, Oct. 5, 2001.

Gutierrez, Geronimo 2004. "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.

Graham, Bob 2001. "A landmark bill that will bolster security at America's deepwater ports passed the Senate by voice vote today." Press release issued December 20, 2001. Downloaded March 20, 2002 at: http://graham.senate.gov/pr122001.html

Halifax Daily News 2003. “A North American Perimeter may be Canadian Business’s Only Hope,” *The Halifax Daily News*, February 16, 2003.

Hite, Randolf C. Testimony for Oversight Hearing: US VISIT- A Down Payment on Homeland Security.” House Committee on The Judiciary, March 18, 2004.

Hufbauer, Gary and Gustavo Vega-Canovas 2003. “Wither NAFTA: A Common Frontier?” in Peter Andreas and Thomas J. Biersteker, *Rebordering of North America: Integration and Exclusion in a New Security Context* (London: Routledge,2003).

ICAO 2003. “Biometric Identification to Provide Enhanced Security and Speedier Border Clearance for the Travelling Public,” International Civil Aviation Organization, PIO/2003 (28 May 2003). Downloaded Nov. 20, 2003 at http://www.icao.int/icao/en/nr/2003/pio200309.htm

Jacobs, Janice L. 2003. “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.

Koslowski, Rey 2004. “Homeland Security and the Globalization of Border Controls,” International Studies Association (ISA), Montreal, Mar. 17-20, 2004.

Koslowski, Rey 2004a. “International Cooperation on Electronic Advanced Passenger Information Transfer and Passport Biometrics,” International Studies Association Meeting, Montreal, March 17-20, 2004.

Larrabee, Richard M. 2002. Statement at hearings on “Container Security” before the House Transportation and Infrastructure Subcommittee, Subcommittee on Coast Guard and Maritime Transportation, United States House of Representatives, Washington, DC, March 13, 2002.

McMahon, Fred 2001. “Perimeter Puzzle,” *Frazer Forum*, December 2001.

MITRE, 2000. “MITRE helps U.S. Customs modernize its business systems,” *MITRE Matters*, September 2000. Downloaded July 1, 2001 at: http://www.mitre.org/news/matters/09-00/mm_09-00_6.shtml

Mulroney, Brian 2001. “Notes for an Address by the Right Honorable Brian Mulroney,” *NAFTA at 10: Progress, Potential and Precedents*, Washington, DC, December 9-10, 2002.

Myers, Deborah Waller 2003. “Does ‘Smarter’ Lead to Safer? An Assessment of the Border Accords With Canada and Mexico.” *MPI Insight* Migration Policy Institute, June 2003, No. 2.

Ohmae, Kenichi 1990. *The Borderless World: Power and Strategy in the Interlinked World Economy* (New York: Harper Business).

Passport Office 2004. “Passport Office Responds to Auditor General’s Report,” Press Release, #49, Passport Office, Department of Foreign Affairs and International Trade, Canada, March, 30, 2004.

Passel, Jeffrey S., Randy Capps, and Michael Fix 2004. “Undocumented Immigrants: Facts and Figures,” Urban Institute Immigration Studies Program, January 12, 2004. Downloaded on Mar. 20, 2004 at: http://www.urban.org/Template.cfm?Section=Home&NavMenuID=75&template=/TaggedContent/ViewPublication.cfm&PublicationID=8685

Pfister, Bonnie 2004. “Regular Border-Crossers Now Are Off the US-VISIT Hook,” *San Antonio Express-News*, March 13, 2004.

Powell, Colin and Tom Ridge, Letter to Jim Sensenbrenner Jr., Chairman, Committee on the Judiciary, House of Representatives, Mar. 17, 2004. Downloaded Mar. 29, 2004 at: http://www.house.gov/judiciary/ridge031704.pdf

Simpson, Glenn R., David Crawford and Keith Johnson, “Crime Pays, Terrorists Find: Group in Europe Smuggles Immigrants and Forges Passports,” *The Wall Street Journal*, April 14, 2004.

Stout, David 2004. “U.S. Extends Fingerprinting Rule to Millions More Visitors,” *The New York Times*, April 2, 2004.

Swarns, Rachel L. 2003. “Passport Deadline Extension Is Sought,” *The New York Times*, March 25, 2004.

Toronto Star 2001. “Italian Court Frees Canadian Suspect,” *Toronto Star*, Nov. 16, 2001.

U.S. Customs 2002. “U.S. Customs Service Launches Customs-Trade Partnership Against Terrorism" Press release, April 16, 2002.

U.S. and Canada 2003. “Smart Border Action Plan Status Report,” Office of Deputy Prime Minister Manley and DHS Press Office, Oct. 3, 2003.

Wallsten, Peter 2004. “Kerry's stances on Cuba open to attack,” *Miami Herald*, Mar. 14, 2004.

White House 2002. “Fact Sheet: Border Security,” The White House, Jan. 25, 2002. Downloaded on Jan 27 at: http://www.whitehouse.gov/news/releases/2002/01/20020125.html

White House 2002a. “Action Plan for Creating a Secure and Smart Border:
U.S. and Canada,” Press Release, Office of Homeland Security, December 12, 2001 Downloaded March 20, 2002 at: http://www.whitehouse.gov/news/releases/2001/12/20011212-6.html

White House 2002b. “Smart Border: 22 point agreement, U.S. - Mexico Border Partnership Action Plan,” Downloaded April 20, 2002 at: http://www.whitehouse.gov/infocus/usmxborder/22points.html

White House 2002c. "National Strategy for Homeland Security" Office of Homeland Security White House, issued July 16, 2002. Downloaded on Jan. 25, 2002 at: http://www.whitehouse.gov/homeland/book/index.html

Ziglar, James W. 2002. "Testimony of James W. Ziglar Commissioner Immigration and Naturalization Service, Before the Committee on Appropriations Subcommittee on Commerce, Justice, State and the Judiciary, United States House of Representatives, Concerning the President's FY 2003 Budget Request." March 7, 2002 Downloaded November 20, 2003 at: http://uscis.gov/graphics/aboutus/congress/testimonies/2002/zig030702.pdf