RAND

INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore RAND Infrastructure, Safety, and Environment

View document details

Border Control

K. Jack Riley
Associate Director of RAND Infrastructure, Safety, and Environment
The RAND Corporation

The borders of the United States can be conceptualized as four segments, or points of entry. Three segments—airports, ports, and guarded land points—are official. The fourth—unguarded land borders and shoreline—is unofficial and is used primarily by migrants, smugglers, traffickers, and perhaps terrorists. Each segment is to some degree porous, because of the volume of activity and the amount of physical space that must be protected. Physical space is particularly important at unofficial points of entry.

The need to improve control over the airport border was highlighted dramatically by 9/11, but the attacks also indicated a need for increased control over the other segments. Meeting that need will be complicated and probably expensive and will necessarily involve many "stakeholders," including foreign allies and trading partners, the private sector, and local governments that have a substantial interest in fees and revenues from ports and airports. This chapter reviews the main policies that have recently been created to strengthen our borders and suggests possible future issues.

THE PROBLEM OF BORDERS

The United States has more than 100 international airports, through which some 88 million foreign visitors pass annually. It also has numerous major ports; for instance, Los Angeles and Long Beach

together constitute one of the world's largest container port facilities, handling approximately half of the seaborne trade entering or leaving the country. Every day more than 16,000 large shipping containers arrive at American ports. Also, the United States protects thousands of miles of land border with Canada and Mexico. Daily truck and passenger traffic at key land ports of entry, such as Detroit (Michigan), Vancouver (Washington), and San Diego (California), numbers in the millions.

The borders of the United States serve many vital functions. All legitimate cargo trade passes over these borders, generating customs and other revenues and duties. In this sense, the borders facilitate the flow of trade, which is increasingly important to the American economy. Borders are also a "choke point" for monitoring the arrival and departure of people. Although 9/11 necessarily focused our attention on terrorists seeking to enter the country, an equally challenging issue is appropriate action against people who have overstayed their visit to the United States. Currently, there are orders of deportation for some 400,000 people who are thought to have absconded and to be living here illegally.

As noted above, the volume of activity at the borders makes control very difficult, and the numerous stakeholders in the processes of control complicate the issue. Even in the atmosphere of caution that has developed since 9/11, other trends are putting strains on borders. For example, many manufacturers and retailers now use the "just-in-time" strategy: to reduce the costs of carrying and storing inventory. They want intermediate and retail goods delivered at the last possible moment. This business model has been facilitated by steep drops in shipping costs and by improvements in efficiency during the last two decades.[1]

An additional complication is that nobody "owns" the borders or segments. Despite the creation of the Department of Homeland Security (DHS), many federal agencies still have a role in border security, and many state and local governments have a role in financing and regulating border segments, particularly ports and airports. Also, private companies such as airlines, truckers, container shippers, and manufacturers—as well as companies whose employees travel over these borders—are stakeholders. These firms care about what the security procedures are and whether private firms are expected to pay for them directly or indirectly. Perhaps

less obviously, various industry, labor, and trade associations have a role in determining work rules and dealing with related issues. Last but not least, there are the interests of our allies and trading partners.

THEMES OF BORDER SECURITY AFTER 9/11

Shortly after 9/11 the authorities took specific steps to improve border security. These programs are discussed in more detail below. Broadly, however, the post-9/11 philosophy has had two important themes:

1. *It is beneficial to push the border out*. After 9/11, security at the border was seen as necessary but insufficient. Accordingly, there was a strong effort to move certain security operations farther offshore to prevent threats from reaching our borders. Examples include requiring advance information on cargo and passenger manifests, positioning Customs and Border Protection (CBP) personnel at overseas ports, and developing means to track stolen passports and to make passports and visas tamper-proof or at least tamper-resistant.

2. *"Profiling out" reduces noise and focuses resources on trouble spots*. All programs that profile out have a common feature: identifying trustworthy people or entities that will be allowed to circumvent routine inspections (though, typically, not random inspections). At land borders, for example, Canadian and U.S. officials have a program called NEXUS that allows travelers who have passed a background check to bypass routine inspection lines. The Customs-Trade Partnership Against Terrorism (C-TPAT), under which manufacturers self-certify their security procedures for goods shipped to the United States, gives this commerce easier access into the country.

We will now consider specific procedures at the four border segments.

AIRPORTS

Because airplanes were used as weapons on 9/11, and because of al-Qaida's well-documented fascination with attacking planes and

using planes for attacks, the security of airplanes has been a high priority.

However, securing the air border segment involves more than securing aircraft. Of the millions of foreigners who visit the United States each year, a few may intend to plan or facilitate terrorist attacks. They may travel with stolen or falsified passports, or they may enter the country using legitimate passports and visas and then not leave when required. A significant aspect of border security is preventing such people from entering the United States. Following are some major changes that have been implemented at airports.

Airport and Airline Security Measures

Many security measures at airports and on aircraft can be considered extensions of border protection. They include air marshals, CAPPS II, screening of baggage and passengers, and NORTHCOM.

Air Marshal Program[2]

In November 2003 responsibility for the U.S. Federal Air Marshal Service (FAMS) was transferred from one component of DHS, the Transportation Security Administration (TSA), to another component—Immigration and Customs Enforcement (ICE). FAMS agents are trained for surveillance, deterrence, and combat to protect American flights.

Computer-Assisted Passenger Prescreening System (CAPPS II)[3]

Responding to opposition from the travel industry, from advocates of privacy and civil liberties, and from other groups,[4] Secretary Ridge announced in June 2004 that CAPPS II was being abandoned. The system had been intended to verify travelers' identity and assess risk by checking passengers against ''watch'' lists provided to airlines by the government. CAPPS II would also have flagged suspicious patterns of purchasing and travel, such as buying a one-way ticket or paying in cash, as well as passengers with certain outstanding criminal warrants. Under Secure Flight, the replacement for CAPPS II, airlines will forward passenger data to TSA for comparison against watch lists. Secure Flight will not target

passengers with outstanding criminal warrants and will not use statistical analyses to predict which passengers may be terrorists.

Screening of Checked Baggage

The Aviation and Transportation Security Act passed by Congress in November 2001 required all airports to screen all baggage checked by passengers; the date for compliance was 31 December 2002. The measure was intended to prevent terrorists from concealing an explosive or incendiary device in checked baggage and detonating it during a flight. Early in 2004, GAO reported that TSA had "collected limited performance data related to its baggage screening operations" and that "TSA deployed Explosive Detection Systems and Explosive Trace Detection equipment to all airports to screen checked baggage...[but] TSA has been unable to fully utilize this equipment to screen 100 percent of checked baggage due to screener shortages, and equipment out of service for maintenance and/or repairs."[5] Thus although airports appear to be meeting the requirement for screening checked baggage, there is concern about the cost and efficiency of the methods they are using.

Screening Passengers and Carry-on Luggage

The nearly simultaneous bombings of two Russian airplanes in August 2004 renewed concern about terrorists' ability to smuggle explosives onto flights. Certain explosives, such as the hexogene used in these two bombings, do not show up well under ordinary gamma-ray screening and may be easily concealed in luggage. Currently, several American airports, including those at San Diego and Tampa, are testing portals that use small blasts of air to dislodge trace particles of explosives. The particles are siphoned through a vacuum to laboratory equipment that rapidly compares the air sample with molecular-weight profiles of explosives. At least two firms, General Electric and Smiths Detecting, make such equipment. The equipment is also being tested at the Statue of Liberty in New York City.

Northern Command (NORTHCOM)

This was developed after 9/11 to fill a security gap in civil aviation—the inability to force down the flights that were used in the terrorist attacks.[6] Previously, American armed forces had focused primarily on flights, and threats, originating outside the country and had

monitored relatively few civilian flights—partly because of radar limits and partly because there was no formal communication link to the Federal Aviation Administration (FAA) in the event of an emergency involving civil aviation.[7] NORTHCOM now monitors 100 percent of civil aviation traffic and maintains a direct link to FAA. Most significantly, NORTHCOM also has the authority to shoot down, as a last resort, flights that appear to threaten targets in the United States. According to press reports, NORTHCOM came perilously close to exercising this authority when a private plane carrying the governor of Kentucky (who was on his way to the funeral of the former president Ronald Reagan) failed to transpond on appropriate frequencies as it approached National Airport.[8]

Passengers' Entry and Exit

Perhaps the most far-reaching change in border controls is U.S. Visitor and Immigration Status Indication Technology (US-VISIT).[9] To speed up the comparison of arriving passengers against watch lists, US-VISIT captures electronic fingerprints, a digital photo, and visa and passport information from these passengers. The system was first tested in Atlanta in late 2003 and became operational at all 115 international airports in the United States on 5 January 2004. Simultaneously, it was introduced at 14 major seaports served by cruise liners.[10] US-VISIT can also be used to assess the extent of visa overstays and to track departures. At several locations, exit kiosks are being tested; foreign visitors check out through these kiosks as they leave the country. The increased monitoring of arriving and departing foreign travelers is a fundamental change in U.S. policy.

A related element is the U.S. Visa Waiver Program (VWP). Twenty-seven countries—mostly European—are part of VWP. Citizens of these countries do not need to have visas for most travel to the United States. Initially, these countries were exempt from US-VISIT: their residents were not fingerprinted or photographed. However, at the end of September 2004 residents of VWP nations were required to adhere to US-VISIT procedures. In addition, to remain eligible for VWP, participating nations were required to provide their citizens with machine-readable passports by 26 October 2004 and biometric-enabled passports by 26 October 2005.[11] The latter requirement was originally intended for 2004, but it was delayed

until 2005 because of objections by the European Union (EU) and many member nations. Actually, as of this writing many European leaders thought that EU would not meet the 2005 deadline and expected another postponement.[12]

Monitoring of visas and exits is a critical element of security, as the 9/11 Commission noted in its report on travel by terrorists.[13] The commission pointed out that all 19 of the terrorists in the attacks on 9/11 had violated one or more provisions of U.S. immigration and visa laws:

> One [attacker]...overstayed his visa by less than six months. Without an exit system in place at the border tied to law enforcement databases, there was no way to establish with certainty that he remained in the United States. Thus, there was no risk that his immigration law violations would be visible to law enforcement, and there was no risk of immigration enforcement action of any kind.[14]

The report also found that before 9/11, all aspects of entry and exit enforcement were weak and uncoordinated and had been given a low priority. This included the State Department's consular procedures for visa management and enforcement activities by the Immigration and Naturalization Service (INS), now the U.S. Immigration and Customs Enforcement.

Airline Cargo

Carry-on bags and checked luggage are screened or manually inspected before being loaded onto planes; in contrast, the vast majority of cargo is not inspected before loading. Airport officials estimate that less than 10 percent of all this cargo is physically inspected, and most airports lack the equipment to conduct inspections, especially of large containers. As with port facilities (discussed below), there is considerable concern that mandated inspections would place an undue financial burden on the $4 billion airline cargo industry and reduce the competitive advantage—speed—that air cargo has relative to other modes of transportation.

Certain programs, such as the Known Shipper Program, which screens companies that send cargo, are designed in part to reduce the need for inspecting all air cargo. The Known Shipper Program is analogous to the Customs-Trade Partnership Against Terrorism (C-TPAT, also discussed below). The Senate passed a bill that would

eventually require all cargo loaded onto passenger jets to be inspected. However, the House has yet to complete action on a similar bill. Some congressional observers believe that this is one of the biggest gaps in border security.

Gaps in Air Border Protection

Substantial progress has been made in securing the air border. The probability of another attack like those of 9/11 has been reduced by reinforced cockpit doors, the arming of some pilots, the presence of air marshals, and increased awareness on the part of passengers. Our ability to identify potential terrorists by using watch lists has also improved—although these security measures are by no means foolproof.

The most serious gaps in air border security appear to be in air cargo and the screening of passengers. Air cargo constitutes a substantial issue: screening it involves complicated problems of logistics, space, cost, and accuracy.

The other serious gap is in screening passengers and their carry-on luggage for explosive devices. Certain explosives are difficult to detect with ordinary screening mechanisms: some do not show up clearly; others, such as hexogene, look like ordinary harmless liquids and so are easily disguised. It seems inevitable that, eventually, airports will be required to have systems capable of detecting the ''vapor signature'' of traces of explosives on passengers and carry-on luggage. As mentioned, promising systems are currently being tested in several airports around the world; but until such systems are deployed, we will have to rely on the existing, unsatisfactory methods.

PORTS

When goods arrive at an American port, they are typically off-loaded at an intermodal transportation hub (on or near the port facilities) and are then transferred to rail cars and trucks for distribution throughout the United States. An attack *through* a port could be devastating, depending on the target. Terrorists could use the ports as a point of entry and deliver a weapon to virtually any place in the country. For example, the ports of Los Angeles and Long Beach together send goods to more than 400 of the nation's 435 congressional districts.

An attack *on* a port—and especially several such attacks occurring simultaneously—could also disrupt the American economy. Ports tend to be large and sprawling, so it is unlikely that any attack would destroy a port's infrastructure. But an attack could disrupt a distribution node for a considerable time and would probably lead to a slowdown at all ports until security measures were reviewed and upgraded.

The consequences of a slowdown undertaken for purposes of security are potentially severe. For example, the port of Los Angeles alone handled more than $140 billion in goods in 2003. How quickly would the costs of port closures mount up? There are at least two cases that provide information about this. In 2002 a brief lockout of longshoremen at ports in the western United States was estimated to have generated losses exceeding $1 billion per day. Given that this lockout was to some degree predictable (the labor dispute was widely publicized, and both sides had indicated their intentions), it could be argued that the losses from a surprise terrorist attack would be even larger. For example, it seems highly likely that after a terrorist attack, the movement of goods would be considerably slowed by increased inspections or by decreased efficiency resulting from damaged infrastructure. Such requirements did not result from the lockout. Second, a consulting firm conducted a ''tabletop exercise'' in 2002 that explored the consequences of a terrorist attack through several ports.[15] The Booz-Allen game generated several lessons, including the realization that emergency postevent security measures were not sustainable and that the restart and rebound capabilities of the port system were unknown.

Below are some major port-related security efforts.

Security of Port Facilities and Associated Infrastructure

The most important legislative step has been the passage of the Maritime Transportation Safety Act of 2002 (MTSA), which primarily addresses the physical security of ports and ships. MTSA is designed to help prevent breaches of maritime security, and to enable recovery from those that cannot be prevented. Among other requirements, it required facilities and ships to develop security and response plans.[16] The U.S. Coast Guard (USCG), a part of DHS, is the primary executive entity for MTSA.

Security of Trade Processes

Whereas MTSA and USCG focus primarily on the physical infrastructure of ports and ships, Customs and Border Protection (CBP) focuses primarily on the process of shipping and moving goods. CBP's overarching objective, with regard to homeland security, is to enhance security within a framework that facilitates the international movement of goods. CBP has led to significant changes in the thinking about security of the supply chain, and how the impact of these changes will be felt for many years to come.

Container Security Initiative

The extension of the borders has several aspects. Container Security Initiative (CSI) combines the presence of CBP personnel with the use of intelligence and other information to identify containers and ships for screening at the port of origination. It consists of four core elements:[17]

1. Using intelligence and automated information to identify and target containers that pose a risk of terrorism
2. Prescreening such containers at the port of departure—i.e., before they arrive at U.S. ports
3. Using detection technology to quickly prescreen these containers
4. Using "smarter" containers that give evidence of tampering

The first stage of CSI, which was implemented in 20 major world ports, covered nearly 70 percent of container traffic entering the United States. With the subsequent addition of other ports, more than 80 percent of the containers reaching the United States are covered by CSI procedures.

Customs-Trade Partnership Against Terrorism

In addition, CBP developed Customs-Trade Partnership Against Terrorism (C-TPAT), a joint initiative by government and business to build cooperative relationships that will strengthen the overall security of supply chains and borders. C-TPAT allows manufacturers and shippers to conduct a security self-assessment and implement a security plan that eases the entry of their goods into the United States.

By May 2003 more than 3,000 importers, carriers, freight forwarders, and other organizations had begun participating in C-TPAT.[18]

Remaining Issues at Ports

It is difficult to pinpoint gaps in the security of ports and supply chains, because to date there has been no comprehensive evaluation of security measures in these areas. As a result, there is very little evidence about how the different elements of security work together; how much security the measures actually provide; or what impact they have on the timing of movements of goods, on synchronization with links to other modes of transportation, or on just-in-time deliveries of manufacturing goods. Given the complexity of international trade and its importance to the U.S. economy, such an evaluation should be undertaken soon, while there are still opportunities to shape and refine the security program.

Even the costs and benefits of individual security programs are not clear. For example, are we better off using intelligence to target containers for inspection or randomly selecting them? What percentage of cargo should we try to screen? There are thousands of facilities and vessels that have had to develop security plans under MTSA, but many of these plans have not been evaluated. Similarly, verifying the accuracy of security self-assessments conducted under C-TPAT is problematic.

The basic issues of security are complicated by the issue of payment: it remains unclear who should bear the burden of upgrading security. Some European officials have objected to CSI, arguing that it fosters security competition among ports, putting small ports at a disadvantage. More generally, ocean shipping is highly competitive and cost-sensitive. Many elements of the private sector are reluctant participants in security upgrades.

The models of security used in ports vary widely. Some ports use local police; others maintain their own forces. The consequences of these different models are not clear. Moreover, whereas workers in aviation are accustomed to carrying identification and to encountering a great deal of visible security, the labor force in ports tends to resist such measures. For example, some staff members have objected to conducting background investigations of port workers.

Also, we know little about the fault tolerance of ports—the ability of the port and supply chain to resist system failure in the event of a disruption—or about resilience: how quickly the stopped system is able to return to normal operations.[19] Fault tolerance is a function of hardness (the resistance of the system to attack), shock absorption (the ability of the system to accommodate the disruption in its locality), and shock dispersion (the ability of the system to dissipate the shock through a network). Resilience, the system's ability to recover after it has failed, is measured by the time until a backup system starts functioning, the time until full capacity is restored and sustainable, and the time to clear all backlogs. We have little experience to help us understand how fragile the international supply chain would be in the face of an attack, and what it would take to reestablish the chain. Contingency planning in this area is important, and policies that promote fault tolerance and resilience should be explored.

REGULATED LAND BORDERS

Mexico and Canada offer dozens of land points of entry into the United States. Some border crossings, such as the one between Windsor (Ontario) and Detroit, are among the busiest in the world. Immediately after 9/11, the borders with Mexico and Canada were, for all practical purposes, closed. Federal officials rushed the National Guard and other security personnel to border crossings. Land crossings into the United States took hours longer than usual, affecting the movement of commerce and the production of import-dependent goods. Generally, this slowdown lasted for only a few months. However, this short-term disruption raised many longer-term issues that are still being addressed.

Border Trade and Commerce

Mexican maquiladoras are an example of the longer-term stakes of border security. *Maquiladoras* are factories, producing a wide variety of goods for export to the United States, that operate in Mexican territory but near the United States. They rely on Mexican labor that is cheap by U.S. standards but well-paid by Mexican standards. In the last decade maquiladoras have lost ground to Chinese manufacturers who have access to a larger, even less expensive labor pool

and who have benefited from a tremendous decline in shipping and logistics costs. Maquiladoras recognize the need for increased security, and many border groups have experimented with or proposed such methods as Web-enabled cameras to monitor manufacturing and the loading of goods onto trucks; credentialed drivers, with satellite tracking of trucks to identify deviations from prescribed (and randomly selected) routes; electronic truck locks that can raise an alarm if improperly accessed; and FAST lanes[20] that allow for more rapid movement of goods over the border. The fear is that the cost of security measures may put Mexican manufacturers at a further disadvantage relative to the Chinese, but that ignoring security will preclude sales to the U.S. market. Maquiladoras are emblematic of the larger issues at stake in port security.

Smart Border Initiatives

The short-term consequences of the slowdown at land borders after 9/11—combined with fears about the impact of security measures on costs and jobs—led to the development of ''smart border initiatives'' with Canada and Mexico.

- ◆ *Canada*: In December 2001 the United States and Canada signed a 30-point border action plan, addressing the secure flow of people and goods, secure infrastructure, information sharing, and coordinated enforcement. The two countries are using dedicated NEXUS lanes that speed prescreened, preapproved, low-risk travelers and goods over the border. Once these travelers and goods have passed rigorous security checks and have provided biometric data for identification, they may cross the border without routine customs and immigration questioning, although they are still subject to random inspection. As of July 2005, NEXUS operated at over a dozen U.S.–Canadian border locations.
- ◆ *Mexico*: In February 2004 Secretary Ridge and Mexico's Secretary of the Interior Santiago Creel signed a ''2004 U.S.–Mexico Action Plan for Cooperation and Border Safety,'' intended ''to improve border safety and security along our shared border in order to prevent migrant deaths and combat

organized crime linked to human smuggling and trafficking."[21] Ridge and Creel also announced their intention to expand another program—Secure Electronic Network for Traveler's Rapid Inspection (SENTRI)—to six land ports accounting for 90 percent of border crossings; and CBP expanded the number of FAST crossings on the Mexican border from seven to 14.

Technology

CPB agents have begun testing a Pulsed Fast-Neutron Analysis (PFNA) system that lets border teams see individual contraband items in large cargo vehicles.[22] PFNA is similar in principle to radar and magnetic resonance imaging (MRI) but creates three-dimensional views and can label the specific content of the cargo by comparing the collected gamma-ray signature with a library of signatures. An inspector would thus be able to guide or refine searches using the visual image along with knowledge about the specific type of contraband. A future demonstration for aircraft cargo scanning is planned.

PFNA is one of several promising technologies that could allow more cargo to be scanned more cheaply and efficiently at borders. Other methods in use are X-ray scanning and gamma-ray scanning (to develop an image of a container's contents), radiation detection, and manual searching. However, additional refinements or breakthroughs are needed before any of these technologies can be used to scan a significantly larger fraction of incoming cargo, vehicles, or passengers. The three issues that must be addressed are as follows:

1. *Increasing the scanning rate*: Faster scanning will allow a greater proportion of cargo to be inspected without creating bottlenecks at the border.

2. *Lowering the cost of equipment*: Cheaper equipment cost will reduce the security tax that scanning imposes on commerce.

3. *Reducing false positives*: Reducing the number of false positives will further reduce the size of the security tax by decreasing the need for expensive, time-consuming hand searches.

Unresolved Border Issues

The remaining issues in land border security are much the same as in port security. It is difficult to know how much security we should be paying for, because little can be definitively said about how effective individual measures are. Our national experience with controlling illicit drug imports (discussed below) suggests that border enforcement is at best a weak deterrent. Increased border enforcement has led drug traffickers to find new smuggling routes and to develop methods that are more difficult for government authorities to police. Similar adaptations by terrorists can be expected.

Although terrorists' behavior will not be static in the face of increased border enforcement, several steps can be taken to make enforcement more effective. In particular, it seems important to invest in developing faster, cheaper, more reliable screening technologies. It would also be prudent to investigate whether the "smart border" procedures with Canada and Mexico will work as planned in the event of another attack. An untested assumption is that NEXUS, FAST lanes, and other programs will keep commerce flowing (or enable a rapid restart) after a disruptive incident. This assumption should be tested with games, simulations, and other exercises that can suggest unanticipated issues.

UNREGULATED LAND BORDERS

At this writing, elected officials and others had recently warned the public about al-Qaida's efforts to evaluate and defeat unguarded portions of the U.S. border,[23] which are primarily the responsibility of the Border Patrol. The Border Patrol uses fencing and other measures at key crossings, although there is evidence that such measures simply displace illegal crossings and activities to unguarded portions of the border. The Border Patrol supplements its efforts in the unguarded areas with unmanned aerial vehicles (UAVs), helicopters, and fixed-wing aircraft. The aerial methods are often used to direct land-based teams to trouble spots. In addition, the Border Patrol has been supplemented by the U.S. military. For example, marine reservists support the Border Patrol by flying helicopters equipped with sophisticated radar to search for illegal border crossings.

Adding to the complexity of this situation are certain factors related to our enforcement capabilities:

◆ *We have limited space for detention and limited capability for deportation*. At present, the U.S. government lacks the capability to handle deportations of convicted criminals who are being released from U.S. prisons and jails.

◆ *We have limited enforcement capacity*. This is particularly true of the borders themselves, where there are few immigration control personnel.

◆ *We do not have extensive cooperation with state and local enforcement agencies*. The first two problems necessitate cooperation with state and local agencies, but many such agencies have policies against arresting or detaining suspects simply on the basis of immigration status. That is, unless there are other indicators (such as an outstanding criminal warrant unrelated to immigration) local police must let such suspects go.

Congress, DHS, and other government entities have developed various responses to address these shortcomings. They include the following approaches.

Border Patrol

In 2003, the U.S. Border Patrol apprehended more than 900,000 illegal immigrants at the border. This figure does not include any who were deterred, were sent back, or made it over the border. Officials estimate that for every apprehension at the border, there may be as many as four successful illegal crossings.

The Border Patrol uses a wide variety of equipment and methods, such as fences and barriers around points of entry, observation towers that increase sight lines along a fence, and infrared cameras and other devices to make observation possible around the clock and in all kinds of weather.

In August 2004 DHS granted the Border Patrol a significant new power—to deport illegal aliens directly. Before that, all apprehended illegal aliens were allowed a hearing before an immigration judge; this process often took a year or longer and thus required a significant amount of detention space, or the release of

aliens before the hearing. The new rule will apply primarily to the land borders with Mexico and Canada, because the authority to deport suspects, without judicial review, who are apprehended at airports and seaports, had already been granted in November 2002. The land border was seen as a necessary extension, given the volume of activity there.

In the post-9/11 environment, the Border Patrol reports concerns about its ability to secure borders. T. J. Bonner, president of the National Border Patrol Council, has remarked: "By a two-to-one margin, the protectors of our nation's borders do not believe that they have been given the proper tools, training, and support to be effective in stopping potential terrorists from entering the country and protecting it from terrorist threats."[24]

Problems of border control and illegal immigration have spawned several private and grassroots border patrol efforts. Perhaps the largest is the Minuteman Project, which claims more than 1,000 patrol volunteers who are "doing the jobs Congress won't do."[25]

Clear Law Enforcement for Criminal Alien Removal

Congress has proposed the Clear Law Enforcement for Criminal Alien Removal (CLEAR) Act, which would offer incentives to law enforcement agencies to increase their participation in the removal of aliens. Currently, many law enforcement agencies below the federal level have a policy of assisting immigration enforcement only if the immigration offense is accompanied by another criminal offense; otherwise, these agencies will not take action.[26] CLEAR, if enacted in its present form, would authorize state law enforcement agencies "to investigate, apprehend, detain, or remove aliens in the United States." Some commentators consider CLEAR misguided, arguing that it is superfluous (simply duplicating existing authorities), that it could distract the police from routine law enforcement, and that it could undermine immigrants' trust in law enforcement.[27] Others have hailed it as a potential breakthrough, arguing that participation would be voluntary and that the legislation would provide access to training, data, and other resources beneficial to homeland security.[28] Supporters also argue that the services of the 600,000 local law enforcement agents are needed, since there are

only 2,000 federal immigration officers to handle more than 400,000 existing orders of final deportation; and that the participation of state and local law enforcement agencies is needed to create a credible deterrent at the border.

IMPLICATIONS FOR POLICY

The process of securing borders can never be complete, because the environment is too complex and the volume of activity is too great. Thus it is prudent to consider what the future of border security might hold. What trends and what issues of policy are we likely to confront?

Two significant issues stand out. First, as we improve our control of airports, ports, and guarded land borders, there will probably be pressure on the unguarded land borders. The 9/11 Commission highlighted this point in its report. Second, since the borders are in a sense a shared asset (because of commerce and tourism), there will be an increasing need to collaborate on border issues with our allies and trading partners. Therefore, this chapter concludes by discussing next steps.

The Push toward the Unregulated Borders

There are two main reasons for the growing concern about unregulated borders. First, as control over air, sea, and regulated land borders is tightened, there is the suspicion that terrorists will attempt entry at the unregulated border. We have seen such flexibility in the behavior of drug smugglers who seek the path of least resistance.

Second, there is increasing concern about Latin America as a potential recruiting ground for terrorist groups, and as a place where terrorist operatives may hide and from which illegal border crossings and drug smuggling can emanate. This concern is based on the region's history of weak, corrupt governmental and police institutions and lax, intractable border controls.

The suspicion that terrorists will eventually focus on the unregulated land borders is probably well founded. The United States' experience with narcotics trafficking at the borders provides some clues. Despite substantial efforts at control, drug traffickers have proved flexible, innovative, and capable of learning.[29] Decade

after decade, quantities of cocaine, heroin, and marijuana sufficient to meet the demand have reached the U.S. market, as traffickers have adopted new techniques (light planes, small offshore boats, submarines, and individual carriers called "mules") and new routes (through the Caribbean islands, over the land border with Mexico, up to Canada and down to the United States). The drug traffickers have persevered because they have a financial incentive. Terrorists have a fundamentally different motivation, but they too are highly likely to circumvent new security measures.[30]

Also, although the border has played only a supporting role in actions against drugs, its role relative to terrorism is far more significant. Kleiman et al. note that "acceptable leakage rates are much lower for terrorism than for drugs....Stopping 90 percent of the drugs entering the U.S. would be a spectacular success, but letting 10 percent of attempted major terrorist acts succeed would be a disaster." This is a crucial difference between border security against narcotics and border security against terrorism. Controlling narcotics at the border is a relatively narrow policy issue, affecting the relatively few countries that are thought to be the primary sources of drugs. Combating the drug trade remains, principally, a public-sector problem; the private sector has little motivation to assist in it. However, border enforcement against terrorism is a broader-based issue that might affect all of the United States' global trading partners. Moreover, after 9/11 the U.S. government demonstrated its willingness to clamp down on the border and to promote comprehensive, long-term programs such as CSI and C-TPAT that affect trade. Repeated border shutdowns, or new border protection measures, implemented unilaterally by the United States, might cost our allies and the private companies that use U.S. borders billions of dollars in lost revenue. In short, foreign governments and private companies have a far stronger incentive to be partners with the United States in protecting the border against terrorism than in protecting it against drugs.

International Relations

In May 2004 the United States imported and exported some $184 billion in goods.[31] Canada accounted for more than 20 percent of the imports; Mexico for approximately 12 percent; and four members of EU—Germany, the United Kingdom, France, and Italy—for

13 percent. The other countries among the top ten importers to the United States are China, Japan, Korea, and Taiwan. These statistics, which do not count passenger movements or dollars spent in the United States by foreign tourists, underscore the fact that the borders are a significant resource. Millions of jobs in the United States and abroad depend on movement of commerce across the border, and many of our consumer products and industrial inputs are obtained through trade.

Thus it is important to understand how our trading partners have been affected by the changes in border security since 9/11. The following paragraphs review issues that have arisen with Canada, Mexico, and EU.

Canada

According to the Canadian Security Intelligence Service (CSIS), ''With the possible exception of the United States, there are more international terrorist organizations active in Canada than anywhere in the world.''[32]—although Canada itself has suffered few terrorist attacks. Terrorist groups use Canada for fund-raising, mobilizing the diaspora, developing logistical and other support for operations, obtaining weapons, and facilitating transit to and from the United States and elsewhere. Chalk and Rosenau have noted:

> Over the past decade, terrorists linked to Hamas, Hizbollah, Egyptian Islamic Jihad, the GIA, al Qaeda, IRA, the Kurdish Worker's Party (PKK), the Liberation Tigers of Tamil Eelam (LTTE), Babbar Khalsa, and the Dashmesh Regiment are known to have entered Canada—generally posing as refugees—to engage in various front and organizational support activities.[33]

If relations between the United States and Canada are strained by border control, the issue has to do with the refugees who seek asylum in Canada. Canada's asylum system is considered generous.[34] Refugees seeking asylum often arrive with little or no documentation, or forged papers. They are allowed to enter Canadian society while their claims (which are infrequently rejected) are being adjudicated. A substantial proportion of those seeking asylum—estimated to be as much as one-third—come from countries such as Pakistan, Saudi Arabia, Iran, and Algeria.[35] Ahmed Ressamn, the would-be ''millennium bomber,'' entered Canada with a fraudulent passport, claimed asylum, and then failed to show up for his hearing.[36] He subsequently

obtained a Canadian passport through criminal means. He was caught by alert U.S. officials as he attempted to enter the United States. His case is typical in Canada (and in the United States): many outstanding deportation warrants are simply not enforced, because resources are lacking and absconders are hard to track down.

The United States' concern about the Canadian asylum system is understandable, given the very porous border, the high level of activity supporting terrorism in Canada, and the continuous flow of new refugees who may rely on their ethnic compatriots for support and acculturation. Still, despite the potential seriousness of this issue, relations between Canada and the United States do not seem to have been unduly damaged. Indeed, there is considerable collaboration between the two nations on border security.

Mexico

According to the U.S. Committee for Refugees, Mexico granted asylum to fewer than 50 of 2,900 refugees and applicants for asylum in 2003.[37] Moreover, Mexico, unlike Canada, is not thought to have many immigrants or nationals who are active in supporting terrorist activities. There is concern, however, about people who enter Mexico using fraudulent passports and visas, and their subsequent ability to surreptitiously make their way to the United States.[38] To combat these threats, Mexico has imposed additional screening requirements for visas and has established a digital passport security system.[39]

A larger issue between Mexico and the United States is the volume of illegal immigration from Mexico. As noted in "Patterns of Global Terrorism 2003":

> A continuing issue of strategic concern to U.S.–Mexico counter-terrorism efforts is the existence and continued exploitation of long-standing smuggling channels traversing the U.S.–Mexico border. These routes have existed for many years to facilitate movement across the border while avoiding U.S. and Mexican authorities. Despite active and prolonged cooperation by the Mexican Government to address these smuggling routes, many smugglers have avoided prosecution.[40]

Although these issues are complicated and always have the potential for conflict, at this point they are not impeding cooperation on border security between the United States and Mexico.

European Union

The United States' relations with EU have been strained by issues of border protection. Customs and border protection are generally a responsibility of EU rather than of the member nations, but EU is in the early stages of developing and consolidating its federal powers. The United States would generally characterize EU as slow to respond to the security threats and concerns that emerged after 9/11. EU, for its part, would generally characterize the United States' actions as unilateral and nonconsultative. On certain issues, the United States has worked at the bilateral or national level, as opposed to the multilateral or EU level. The issue has become very complicated. For example, EU filed suit in the European Court of Justice to overturn bilateral agreements between the United States and individual EU member states on the Container Security Initiative (CSI). EU won the suit and has since implemented an EU-level agreement with the United States.

There are other barriers to increased cooperation between the United States and EU on border security, although not all these barriers have actually developed in the context of border security:

- *Intelligence*: U.S. intelligence agencies want to be able to predict how European courts will handle intelligence issues. The United States feels that this has not yet been achieved and that much detailed work, some at the bilateral level, must still be done.

- *Law enforcement*: There is little or no "law enforcement" constituency among European nations generally or EU in particular. This creates a sense of imbalance in the relationship, with the United States often pushing enforcement issues.

- *Decision making by EU*: This is a slow process and generally conflicts with progress in the United States, particularly under DHS, which tends to move fast and be focused.

- *Role of the private sector*: The private sector has little involvement in EU's planning, relative to the role of the private sector in the United States. In the United States, the involvement of the private sector in homeland security ensures that initiatives receive extensive attention, lobbying, and resources.

More positively, DHS and EU have increased high-level contacts in an effort to ensure that potentially contentious policy issues are identified as far in advance as is practical and to create additional mechanisms for resolving future disputes.

CONCLUSION

Security at U.S. borders has been significantly increased. Much of policy implemented after 9/11 reflects the principles of ''pushing the border out'' to extend the reach of our security and ''profiling out'' less threatening people and cargo in order to focus on targets that require more scrutiny. These principles have made border control more manageable, though they have by no means resolved certain broader issues of security.

Underlying these themes, however, is the startling realization that we do not know very much about the effectiveness of individual border security programs, or about how various programs work together to affect commerce, costs, and security. The effectiveness of programs such as CSI, C-TPAT, and US-VISIT has not been evaluated. The leaders of such programs, however, are increasingly aware of the need to establish performance standards—for one reason, because representatives of the private sector are concerned about the cost of security.

There is also increasing need for evaluation above the program level, at the strategy level. As we enter the fourth year after 9/11, it is becoming increasingly clear that securing the homeland is expensive and potentially endless. How much we should spend on, say, airline security compared with rail and bus security will become increasingly relevant. We cannot begin to resolve broad issues of resource allocation until we know more about individual programs (such as airline security). Evaluating the effectiveness of individual programs will provide a basis for the more strategic allocation of resources across programs.

Finally, there is a need to develop a road map for investing in technology for border security.[41] Faster, cheaper, more reliable screening technologies are needed. Similar needs arise in many other areas of border security and of homeland security generally. When there is a pressing need for security, there can be an incentive to invest in any—or all—apparent technological solutions, regardless of the

potential payoff. Inherent in technology development, however, is risk. Some technologies are simply not going to reach their expected potential; others will reach it, but perhaps over a time span that will not meet current needs. It is important to structure the investment pattern so that homeland security officials will invest in technologies that address mission-relevant functions and provide essential capabilities.

N O T E S

1. Michael Wolfe, ''Freight Transportation Security and Productivity: Complete Report,'' Long Beach, Calif.: Intermodal Freight Security and Technology Workshop (27–29 April 2002). Wolfe provides details on logistical improvements.
2. For a more detailed review of the marshals' program, see *Aviation Security: Federal Air Marshal Service Is Addressing Challenges of Its Expanded Mission and Workforce, but Additional Actions Needed*, GAO (November 2003); and *Evaluation of the Federal Air Marshal Service*, Office of Inspections, Evaluations, and Special Reviews, Department of Homeland Security (August 2004).
3. The airlines had responsibility for administering the first prescreening program, CAPPS.
4. For opposed opinions, see ''Business Travel Association Applauds GAO Report but Fears Potential CAPPS II Impact on Industry,'' Association of Corporate Travel Executives (12 February 2004); ''CAPPS II: Government Surveillance via Passenger Profiling,'' Electronic Frontier Foundation, accessed at www.eff.org/Privacy/cappsii/background.php on 9 September 2004; and ''Barr Submits Formal Objections to Passenger Profiling System,'' American Conservative Union (30 September 2003).
5. ''Challenges Exist in Stabilizing and Enhancing Passenger and Baggage Screening Operations,'' GAO (12 February 2004).
6. Several GAO reports mention a lack of attention to general aviation as a potential terrorist threat. See, e.g., GAO-03-1150T, ''Progress Since 11 September 2001 and the Challenges Ahead''; and GAO-04-592T, ''Improvements Still Needed in Federal Aviation Security Efforts.''
7. *The 9/11 Commission Report* reviews the positions of FAA and NORAD; see pp. 82–5, 352.
8. Spencer S. Hsu, ''Plane that Caused Capitol Evacuation Nearly Shot Down,'' *Washington Post* (July 8, 2004; p. A1).
9. For an overview, see GAO-04-586, Randolph C. Hite, *First Phase of Visitor and Immigration Status Program Operating, but Improvements Needed* (Washington, D.C.: Government Accounting Office, 2004).
10. US-VISIT is expected to be operational at all land points of entry by the end of 2005.
11. ''Extension of Requirement for Biometric Passport Issuance by Visa Waiver Program Countries,'' press release, U.S. Department of State (10 August 2004).
12. Personal interviews with EU and EC leaders (26–29 July 2004), Brussels, Belgium.

13. *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks upon the United States*, 2004.

14. Ibid., p. 4.

15. Booz-Allen-Hamilton, ''Port Security War Game: Implications for U.S. Supply Chains,'' Executive Summary (2002).

16. Other objectives and requirements included maritime safety and security teams, security assessments for foreign ports, and a common identity card for transportation workers.

17. www.cbp.gov/xp/cgov/enforcement/international_activities/csi/csi_in_brief.xml, accessed 3 September 2004.

18. *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, GAO-03-770 (25 July 2003).

19. Henry H. Wills and David S. Ortiz, ''Evaluating the Security of the Global Containerized Supply Chain,'' TR-214-RC, RAND (2004).

20. Free and secure trade (FAST) lanes. Manufacturers shipping by FAST lanes must agree to many of the security measures mentioned above. Secretary of Homeland Security, ''Fact Sheet: U.S.-Mexico Bilateral Meeting'' (20 February 2004).

21. Ibid. This agreement formalized a 22-point plan announced in March

22. Ryan Singel, ''New Nukes at U.S. Border,'' www.wired.com/news/technology/0,1282,64735,00.html. See also www.ancore.com/ACI-PFNA_brochure.PDF.

23. See, e.g., Brad Olson, ''Terrorists Probing U.S.-Mexico Border, Intelligence Suggests,'' *Corpus Christi Caller-Times* (3 September 2004); and Alan Caruba, ''Is a Terrorist Army Massing in the U.S.?'' *MichNews* (28 August 2004). According to the latter, ''In July, Defense Watch reported that, in Arizona, an area called the Naco Strip has become a primary route of illegal entry by 'significant numbers of Arab-speaking males.' It took a small town weekly newspaper, the *Tombstone Tumbleweed*, to reveal that 'males of possible Syrian and Iranian descent have been detained in the past few weeks.' Since 1 October 2003, 5,510 illegal aliens designated 'Other Than Mexican' (OTM) have been apprehended while crossing the Arizona terrain.''

24. ''How Secure Are America's Borders? Front-Line Border Protection Personnel Speak Out,'' Statement by T. J. Bonner, president of National Border Patrol Council of the American Federation of Government Employees (23 August 2004).

25. Accessed July 25, 2005 at www.minutemanhq.com/project.

26. E.g., refer to LAPD special order No. 71.

27. James Jay Carafano, ''No Need for the CLEAR Act: Building Capacity for Immigration Counterterrorism Investigations.'' Heritage Foundation, Executive Memorandum No. 925, 21 (April 2004).

28. U.S. Representative Charlie Norwood, ''CLEAR Act Pointed to as Solution to Criminal Alien Crisis at House Hearing,'' news release (3 October 2003). According to the release, the bill (H.R. 2671) is supported by the National Sheriffs' Association, the Law Enforcement Alliance of America, the Southern States Police Benevolent Association, and Friends of Immigration Law Enforcement, and by more than 100 members of Congress.

29. For the evolution of drug trafficking, see K. J. Riley, ''Snow Job? The War against International Cocaine Trafficking,'' *Transaction* (1996).

30. Mark A. R. Kleiman, Peter Reuter, and Jonathan P. Caulkins, ''The 'War on Terror' and the 'War on Drugs': A Comparison,'' *FAS Public Interest Report*, (March–April 2002). See Vol. 55, No. 2 for a more complete comparison of drugs and terrorism.

31. Statistics are from U.S. Department of State International Information Programs accessed at www.census.gov/foreign-trade/top/dst/current/balance. html (10 September 2004).

32. ''Operational Programs: Counter-Terrorism,'' Canadian Security Intelligence Service, rev. 9 (August 2002), accessed at www.csis-scrs.gc.ca/eng/operat/ ct_e.html (9 September 2004).

33. Peter Chalk and William Rosenau, *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies*, RAND, MG-100 (2004). See especially pp. 25–31.

34. James Bissett, *Canada's Asylum System: A Threat to American Security*, Center for Immigration Studies (May 2002). Bissett provides an overview of the issues. See also Stephen Gallagher, ''Canada's Dysfunctional Refugee Determination System: Canadian Asylum Policy from a Comparative Perspective,'' *Public Policy Sources* 78 (December 2003) (Fraser Institute).

35. ''Canada's Asylum System: A Threat to U.S. Security,'' Panel Discussion Transcript, Center for Immigration Studies (22 August 2002).

36. *9/11 and Terrorist Travel*, p. 53.

37. ''World Refugee Survey 2003 Country Report,'' U.S. Committee for Refugees. Report, accessed at www.refugees.org/world/countryrpt/amer_carib/2003/ mexico.cfm (10 September 2004).

38. The United States' processing of Mexicans' requests for visas has also been questioned. See United States Embassy press release, ''Temporary Suspension of Visa Processing in U.S. Consulate General in Ciudad Juarez,'' rev. 20 June 2003, accessed at www.fullerton.edu/international/TRAVELVISA/Mexico VisaProcessing.htm (10 September 2004).

39. ''Patterns of Global Terrorism Report 2001,'' Office of Counterterrorism, Department of State (21 May 2002).

40. ''Patterns of Global Terrorism 2003,'' Office of the Coordinator for Counterterrorism (29 April 2004).

41. See B. W. Boehm, *Software Engineering Economics* (New York: Prentice Hall, 1981); L. Putnam, *Measures for Excellence: Reliable Software on Time, within Budget* (New York: Yowder, 1992); Lance Sherry, *Four Habits of Highly Effective Software Development Managers*, Software Development (2001); R. S. Silberglitt and Lance Sherry, ''A Decision Framework for Prioritizing Industrial Materials Research and Development,'' MR-1558-NREL (2002).