Report #05-031

Vulnerabilities along US Borders: A Brief Analysis of Risks Posed by Terrorist, Illegal Weapons and Explosives Traffic through US Borders and Countermeasures for Risk Mitigation

Bakir, N.

CREATE REPORT
Under FEMA Grant EMW-2004-GR-0112

March 14, 2006

Center for Risk and Economic Analysis of Terrorism Events
University of Southern California

Los Angeles, California

This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number N00014-05-0630. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security.

Vulnerabilities along US Borders: A Brief Analysis of Risks Posed by Terrorist, Illegal Weapons and Explosives Traffic through US Borders and Countermeasures for Risk Mitigation

CREATE Report

- THIRD DRAFT -

Preliminary work-in-progress.

Please do not quote, cite, or distribute without the author's consent.

March 14, 2006

Niyazi Onur Bakir
USC Center for Homeland Security (CREATE)
University of Southern California
3710 McClintock Ave., RTH 314
Los Angeles, CA 90089-2902

Acknowledgment

This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE), grant number EMW-2004-GR-0112. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the US Department of Homeland Security.

EXECUTIVE SUMMARY

The attacks of September 11 raised interest in global terrorism and demonstrated vulnerabilities in the American homeland. For the first time in history, homeland security missions were aggregated under a centralized agency by the creation of DHS in 2002. Borders, which serve as a barrier between the American homeland and the rest of the world received more attention. The entire airline industry, importers, shippers and those who travel across the borders have remained on a higher state of alert. The challenge became more apparent as a simple analysis of security status along US borders revealed that terrorists have a variety of options to launch attacks with potentially catastrophic consequences. Security challenges are further exacerbated by the limited nature of resources and lack of clear strategy in allocating them. Since risks cannot be fully eliminated, there is a clear need to determine how to prioritize risks and evaluate the marginal benefit from each dollar spent on risk mitigation.

This project seeks to evaluate alternative policies and technology solutions for protecting our borders against illegal importation of weapons, terrorist infiltration and direct terrorist attacks while maintaining our competitiveness in international trade. The scope of the project covers maritime, land border and aviation security. It is our intention to develop a systems based risk management approach that integrates border security operations and performs comparative risk assessment between different elements of the system to support fund allocation decisions. To this end, a comprehensive overview of threats and vulnerabilities will be made. We will examine alternative strategies, including methodologies for screening and inspecting cargo, and operational improvements that promote participation in trusted shipper programs. We seek to provide a comprehensive examination of the alternative methods for shipping goods into the United States, and a comparison of technology based solutions to deter and detect terrorists and weapons crossing the borders. A particular focus will be on protecting the nation against importation of nuclear materials and weapons.

So far, dollars have been appropriated with minimal risk comparison and recognition of the adaptive nature of terrorist strategies. First, aviation passenger and baggage security, then maritime container security, and recently land border security have attracted a lot of media coverage and public attention, while some of less pronounced risks have been relatively ignored. This report seeks to direct attention to other vulnerabilities along national borders that terrorists can exploit for the next catastrophic strike. In the second chapter, we give an overview of a systems based risk management approach that models the border security as a collection of sub-components that forms a system achieving a common objective. A central decision maker is assumed to choose among a set of investment and policy alternatives, each associated with respective costs of implementation. Benefit of each investment and policy is measured by the reduction in risk exposure of the overall system, rather than the reduction of risk on a particular component. Component risks are interdependent as terrorists formulate their strategies to exploit vulnerable points of defense systems. We believe that this modeling approach will eliminate any investment strategy that allocates limited funds with minimal risk comparison across the whole system. However, we recognize that budgeting decisions are affected by some external homeland security missions not directly related with border security. These external missions such as emergency response capabilities are not directly related with the issues covered in this report, although they have an impact on the terrorism risk profile along borders. Therefore, it may rather serve as a tool to determine the distribution of a fraction of resources appropriated for the homeland security mission.

Three main components in border security are aviation, maritime and land border security. In this report, we make an attempt to summarize all terrorism risks on each main component. In a broad sense, terrorism risks on components and their sub-components fall under one of the following three categories. The first category is direct attack risks on critical components which may be high value targets for terrorists. This risk category exposure is particularly found along maritime borders and in the air. The second category is the

risk of terrorist penetration exploiting gaps in security on a particular component to launch attacks at some inland target. Land border sub-components are particularly exposed to risks in this category. The third risk category is introduction of illegal weapons and explosives to launch an attack elsewhere in the homeland. All components in the border security system have to address this risk as each component has a trade attribute attached. The severity and likelihood of risks and the economic value of risky components determine the criticality of each component and its sub-components.

In the third chapter, we discuss maritime security. Two main components in maritime security are port security and security of US waters. At least in the media, port security is mainly intertwined with cargo security. Loopholes in containerized cargo trade were brought to public attention numerous times. While risks of introducing dirty bombs or illegal weapons are real, we fear terrorists can use other forms of cargo to launch attacks. Another sub-component of port security is port perimeter security. This sub-component is very critical as most critical targets along coasts are close to maritime ports and an attack on either of the targets would halt all the operations along maritime borders. Besides ports, US waterways are vulnerable. Most nuclear power plants and LNG terminals that satisfy energy needs of the economy are on the coast. Furthermore, waterways may be an open path for those who cross borders illegally, or introduce weapons and explosives.

The next chapter is devoted to porous land borders. Each year over a million are apprehended along land borders and an estimated number between 8 million to 20 million illegal aliens are in the United States. Land borders also have two sub-components: ports of entry and between ports of entry. Ports of entry have both a trade component and a traveler component. On the other hand, between ports of entry, we have no trade and no infrastructure, so the Border Patrol’s mission is simply to deny entry to illegal aliens, who may have weapons in possession. Despite the rough natural conditions along land borders, the chance of an illegal crossing is higher between ports of entry. Since the understaffed Border Patrol does not deter illegal aliens from crossing the border, there is a little chance terrorists will be deterred once they find the opportunity to do so.

Before we offer our concluding remarks, we discuss some aspects of aviation security related with border security. We address issues in passenger screening, access to secure areas in airports, baggage and cargo screening and visa issues. Not addressed in this report are issues on general aviation security and airport perimeter security. Security breaches still exist in the air despite the long history of terrorism events with a high number of death tolls.

In this report, we do not address bioterrorism aspects of border security. Also a broad economic analysis of each countermeasure is beyond the scope of this report. There is a potential for identifying case studies on specific vulnerabilities along US borders and evaluation of countermeasures to mitigate associated risks. In specific case studies, we look forward to doing in-depth analysis on potential economic impacts and risk reduction benefits of countermeasures.

Table of Contents

I. INTRODUCTION

The last decade of the twentieth century witnessed a great surge into economic and social globalization. Technological advancements have been the catalyst of this transformation as they have enabled faster information sharing, more reliable communication and integrated world markets. This trend has generally worked favorably for developed nations which could extend influence to new markets through new business initiatives, and bring more jobs and welfare to their homeland. The western cultural diffusion has been sustained as a global trend with the worldwide promotion of capitalism. All aspects of life have become more broadly and deeply interconnected, even for those who have had minimal access to mass media.

On September 11, 2001, we came to the realization that terrorism evil has also gone global, capable of launching attacks in the once impenetrable American homeland protected by natural barriers. Growing American influence, increasing distress in poor countries and lack of economic opportunities have made it easier to get recruits for those who want to change the world system through terrorism. Terrorists have developed the tactical and technological sophistication to launch attacks that could generate mass casualties, disrupting global economy and striking widely spread fear across the world. More and more terrorist groups mushroomed, forming a global network of terrorism posing an asymmetric threat to the United States and the interests of most other developed nations.

In the new era, most of the underlying assumptions of border security have collapsed immediately. We have realized that those who want to harm the United States will attempt to do so by any means possible. As the military might of the United States makes it tactically senseless to wage a conventional war, terrorists have moved forward to exploit other vulnerabilities of the United States. There are plenty of them, particularly along the entire border. As the idea of “Fortress America” has blinded most Americans about gaps in border security, it was not until 9/11 that media and the public warranted attention to this growing threat. Today, post 9/11 efforts to seal up the borders reveal the years of ignorance on the issue.

Terrorists have already exposed the United States in the air. They are reportedly seeking to gain capabilities to exploit other vulnerabilities along maritime and land borders. The National Strategy for Homeland Security and the Homeland Security Act of 2002 served to unify all the stakeholders’ and government agencies’ roles in homeland security under one centralized agency. One agency to protect the homeland works towards an integrated risk management approach to mitigate risks. Effective allocation of resources can be accomplished by following a systems based risk management approach under a centralized decision maker that recognizes the interdependencies between risks and adaptive nature of threats. To this end, we need a comprehensive assessment of current threats, vulnerabilities and critical assets of the economy.

Border security is the underpinning for the nation’s economy and continuity of business. The prosperity that this nation has enjoyed for years rests on properly functioning borders. A major disturbance of border operations has a potential to deliver a serious blow to whole economy. As terrorists shifted their strategy over time from harming solely people to harming economic interests, borders have become targets themselves, besides serving as a protective barrier for the internal targets elsewhere. Accordingly, development of a layered approach to protect against terrorism has become an inevitable strategy. To this end, DHS launched initiatives to extend maritime borders in an effort to develop an extra shield in the homeland security system. However, political barriers, and sovereignty issues made the progress slow, leaving gaps in security.

The trade offs between free flow of commerce and border security make technology and policy decisions more complex than ever. Today, we realize that we need to avoid “too much” security as most security solutions slow trade. There is a need to determine the relation between terrorism risk tolerance and maximum inconvenience that the nation can bear on business continuity. There is a fine balance between those two, and this fine balance can be maintained only if a systems based risk management approach is followed to distribute security dollars. An overall assessment of the threats and vulnerabilities along US borders is key to allocate homeland security grants in parallel to nation's interests rather than political interests. To this end, we expect that this report will feed useful input to grant allocation decisions.

We need to eliminate conflicting objectives of policy makers involved in border security decisions. Roles and missions of each stakeholder should be clearly identified and government, state and local officials should follow their roles and missions to achieve a common goal. Government has to provide incentives to minimize conflicts of interest, so that risk management principles become sole factors in making decisions and implementing various policies. Synchronization of efforts towards serving interests of the nation and countering problems over the long-term is one of challenges that government faces in the future.

This document is organized as follows. Section 2 describes the systems based risk management approach that could be used to model border security decisions given multiplicity of threats, adaptive nature of the adversary and multiple border components. We describe the components of the system and the benefits of integrating border security decisions that affect the probability of failure and the consequence should the failure occur. Sections 3 and 4 are devoted to vulnerabilities along maritime and land borders respectively. The threats and countermeasures to mitigate terrorism risks are outlined. In Section 5, we provide a similar discussion within the context of aviation security. Section 6 presents some concluding remarks.

II. A SYSTEMS APPROACH FOR BORDER SECURITY

The main objective of border security is to minimize casualties and economic losses due to terrorism while ensuring flow of commerce, continuity of business, conserving environment and supporting international partnerships for research, development and education. To this end, a variety of policies are implemented, laws are enforced and human and capital resources are deployed. An ideal border environment would deny entry to all illegal aliens crossing the border, detect all contraband and preclude all potential attack scenarios on critical facilities along US borders without disrupting the integration of this nation with the rest of the globe and undermining the continuity of wildlife. The truth is that we are far from this ideal environment where all risks are eliminated. Furthermore, it will never be possible to fully eliminate all the risks around US borders given limited resources. The solution is to implement a systems based risk management approach that captures the complex relationship between multiple components and their exposure to interdependent risks, deploy necessary resources and mitigate exposure to a nationally tolerable level.

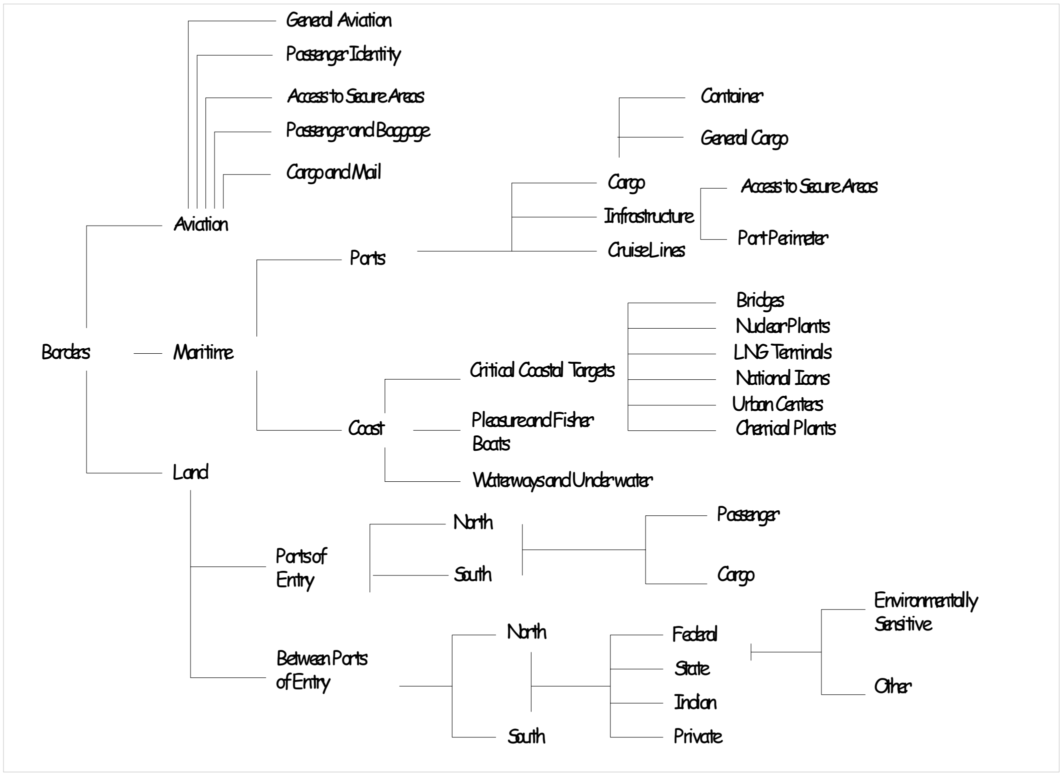
In this document, we are interested in protection of American borders against illegal importation of weapons, illegal penetration of terrorists and protection of targets along US borders. One of the means to launch terrorist attacks is to introduce illegal weapons or explosives into the United States and use them against domestic targets. Borders are clearly the only avenue to achieve this objective. Two confirmed attempts that have been recorded earlier to introduce weapons and explosives strongly suggest that terrorists' may consider options that include illegal border crossings and illegal importation of weapons into the homeland. Illegal border crossings will be a point of discussion in this document inasmuch as they relate to importation or use of weapons or explosives for terrorism purposes. Further, maritime and aviation security are particularly vital for the economic prosperity of the country as many businesses have stakes in airline and maritime operations. Terrorists have expressed their intentions to hurt American economic interests. Accordingly, borders constitute targets for terrorists, and measures have to be taken to prevent potentially catastrophic attacks on these targets.

A. Border Security System

Border security system has three main components; maritime security, aviation security and land border security. Each component constitutes a subsystem with interacting sub-components, each exposed to interdependent risks due to potential terrorist attempts to cross the borders. For instance, land border security has two interacting sub-components; security at the ports of entry and security between ports of entry. Both sub-components are exposed to illegal alien entry and contraband smuggling risks. Terrorists seeking entry into the United States through land borders will make an attempt to violate the law at either of these points. If both risks are relatively mitigated at the ports of entry by deployment of new technology and more border agents, then terrorists will choose to cross borders between ports of entry. This would increase the terrorism risk exposure between ports of entry, hence increasing the probability of failure of this sub-component. A component of the system is said to “fail” if terrorists achieve any of the three objectives: attack a target along borders, successfully import illicit weapons and explosives or penetrate inland without interdiction. We need to develop a model that addresses the interdependencies between component risks and supports investment and policy decisions simultaneously to mitigate terrorism risk.

Figure 1 illustrates the components and the sub-components of the border security system. The sub-components of maritime and land border security are determined more on the basis of their location whereas in aviation security, they represent different aspects of security in commercial and general aviation. For instance, maritime security is analyzed under two main headings: port and coast security. Ports differentiate themselves from other coastal targets with commercial trade volume and passenger traffic they handle. However, there are some overlapping security issues between ports and other coastal targets such as security of waterways and boats sailing in US waters for either recreational or commercial purposes. In this regard, classification under each component does not necessarily induce a disjoint set of risks associated with each sub-component. Depending on the location, level of vulnerability toward a similar threat may differ and is largely determined by the level of resources allocated to counter the threat.

Figure 1 An Overview of the Border Security System



The classification under port security is context based rather than location based. Security of containerized cargo destined for the United States has been arguably the most highlighted vulnerability at seaports both in the media and academic circles. As companies extend their reach to new foreign markets and engage in global supply operations, countries are getting increasingly interconnected through a network of trade relationships. Containers serve as the main medium of transportation in this huge trade network. While containers provide a lot of convenience in unitizing cargo as well as loading and unloading operations, they also provide ways and means to transport illegal contraband. In this regard, containers may be used to introduce illegal weapons or explosives into US. Therefore, terrorist presence in foreign countries with extensive economic ties with US transfers the terrorism risk to American homeland. Container security is not only about monitoring cargo at the maritime ports of entry. Intermodal transportation security, immigration policies, port security at foreign ports of origin, identity of foreign workers loading and screening containers and stakeholders involved in the whole process suddenly become issues of concern for policy makers and terrorism experts in US. A relatively less often pronounced type of vulnerability reveals itself in monitoring of general cargo, which constitutes another sub-component under cargo security.

Economic impacts of a critical seaport closure are measured in billions of dollars. A terrorist plot to halt port operations may involve illegal access to secure areas or launching attack from or to port perimeters. In particular, gaining access rights to secure areas due to gaps in background checks would provide an excellent opportunity for a strike. Similarly, attacks on targets around the ports may render long term port closures if access from either land or sea is restricted as a result of the attacks. Maritime ports also handle traffic of cruise line passengers, which add to the complexity of security check operations.

For land borders, location based classification for sub-components are mainly motivated by the differences in the level of resources allocated, the role of international trade, the specific nature of threat that pertains to terrorist capabilities to violate border laws and functions of law enforcement agencies. Ports of entry have a huge trade component that brings complexities of cargo security into the border security decisions. On the other hand, interdiction of illegal aliens and illegal contraband is an issue at all sections of land borders. Among the three agencies that are directly involved with land border security mission, CBP assumes most of the responsibilities ranging from cargo inspections to interdicting illegal aliens at the land borders. An administrative branch of CBP, the US Border Patrol, is the sole enforcement agency between ports of entry, whereas immigration officers and customs officers of both CBP and ICE have the authority to perform inspections on exported material and aliens seeking entry into the United States.

Air terminals experience a higher proportion of passenger traffic, whereas maritime ports mainly serve as hubs for incoming cargo. For land ports of entry, there is relatively a more balanced mix of cargo and passenger traffic. Unlike air terminals and maritime ports, land borders are not likely to be targets of a terrorist attack. Terrorism risk is rather concentrated around importation of lethal contraband and an illegal terrorist entry. The main challenge for both sub-components of north and southwest land ports of entry is to facilitate legitimate cross-border traffic and interdict illegal contraband at the same time. Conversely, the challenge in the vast stretches of frontier laying between land ports is to stop any form of traffic. Drug traffickers and illegal immigrants are actively using the trails at relatively less monitored sections of the border. The Border Patrol has the legal authority to patrol within 25 miles of the border without any notice to land owners. However, level of terrorism risk exposure depends on actions of authorities holding jurisdiction over the land. This is main reason behind location-based classification under north and southwest between ports of entry. Furthermore, countermeasures in environmentally sensitive areas should adhere to environmental regulations and render minimal interference with the natural habitat.

In the aftermath of 9/11, aviation security warranted huge attention. With the efforts of TSA under DHS, deployment of resources to improve air transportation security has become a priority. Since technology and human resource allocation at nation's airports have been rather uniform, the sub-component classification under aviation security is based on potential security breaches. The classification highlights multiple avenues that terrorists can use to import illegal weapons, hijack airplanes, send bombs on board or enter US illegally. The interdependence of multiple forms of terrorism risks on aviation security sub-components is largely a function of the capability of terrorists to diversify their tactics and focus.

Verification of the identity of passengers flying in commercial airplanes, checking the contents of their baggage and carry-on belongings have been the main focus in aviation security over the years. However, this did not stop 9/11 attacks. All of the hijackers were in legal status and they brought neither weapons nor explosives on board. Their hijacking tactics did not necessitate use of any sophisticated weapons; box cutters and knives were reportedly the only tools used to terrorize the passengers and the flight crew. The immediate response was to expand the list of banned items on board, deploy detection machines, transfer the screening responsibilities to federal workers, and developing new passenger prescreening systems. Despite the progress made to this end, verification of passenger identity, screening of carry-on bags and other luggage remain as the potential vulnerabilities of the airline system.

Among many lessons taught by 9/11 is that any airplane can be used as a weapon in the hands of a pilot with suicidal tendencies. As security measures for commercial airplanes are tightened, a potential copycat attack is feared to involve a private aircraft. These concerns have been justified by the crash of a single-engine plane into a skyscraper in Tampa, Florida[1]. Terrorism threat along the common borders with Canada and Mexico in the form of an aerial attack is commensurate with the general aviation security in both countries as well as air radar surveillance in the United States.

Two overlapping issues in maritime and aviation security are security of cargo and port areas that require special authorization for access. While a relatively higher proportion of air cargo is inspected, the nature of the terrorism threat in the form of an air cargo bomb suggests that the overall risk is no less than that of a maritime cargo. Since the security of cargo of all forms is closely related to supply-chain security, similar countermeasures can be employed to reduce risk of cargo tampering regardless of the route to destination. Unauthorized access to secure areas could introduce another point of vulnerability into flow of cargo and create an opportunity for potential terrorists to bring banned items on board to hijack the aircraft.

Border security management has an analogy with management of a system with multiple components. Components interact with each other and function to achieve a common objective. Every component is subject to random shocks whose interarrival times are governed by a common probability distribution. Each shock to a component is countered with resources available for that particular component. The component survives the shock if sufficient resources are available to counter the shock. Otherwise, the component fails. An example of a shock in this context could be an attempt by a terrorist to cross the border between ports of entry. The “between ports of entry” component fails due to such a shock if the terrorist crosses the border without being apprehended. However, a single component failure may or may not lead to an overall system failure. There is still a probability that the terrorism plot is discovered before the attack is launched by a terrorist who illegally crosses the border. If the system fails, then there will be costs associated with the failure, in both dollars and human casualties.

B. Resource Allocation for Risk Mitigation

In border security terminology, each shock is an attempt to cross the border for terrorism purposes. The system manager has to allocate resources among multiple components to minimize the expected utility of losses. To this end, he distributes total system resources among the components that are translated to countermeasures at the component level. Each countermeasure may serve for reducing likelihood and severity of the shocks.

An investment to mitigate terrorism risks could be made with either technology or human capital. An overall assessment of nation’s terrorism risk profile requires a comprehensive evaluation of investment status across all sub-components of the system. Marginal value of an incremental investment depends on the current status of the system. Marginal value of an extra investment may be low if it offers overlapping benefits to the system. Alternative policies, which include initiatives and regulations, may be treated in the same manner. It should be our goal to avoid resource allocation based on policies that yield overlapping benefits.

The objective is to minimize expected disutility of fatalities and economic losses of terrorism events as well as negative economic impacts of security measures. A central decision maker is implicitly assumed to make the final call. The disutility function is additive in its arguments. In other words, both attributes of the disutility function are preferentially independent.[2] Conservation of wildlife and environment, continuity of research

[1] Vickie Chachere, “Plane Crashes into Tampa Skyscraper”, AP Online, 6 January 2002.

[2] A utility function is additive if and only if its attributes are mutually preferentially independent. For a general discussion on attributes of the utility functions, please refer to Ralph L. Keeney, Howard Raiffa, “Decisions with Multiple Objectives”, Cambridge University Press, 1993.

partnerships and education is not a part of the objective. Instead, they may act as constraints on investment and policy alternatives available. A very effective policy to largely eliminate terrorism risk is to close all ports of entry to incoming cargo and people, hence immediately stopping all cross-border economic activity. However this policy should never be chosen by a central decision maker because of the constraints that require a reasonable level of border trade that feeds the US economy. Similarly, fence building along land borders should be carefully implemented due to its potential interference with natural habitat. In this regard, border security that ensures better environment and efficient transportation of goods across the supply-chain serves national interests. However, the main objective of making borders secure is to minimize negative impacts of terrorism events should they occur.

Resources allocated on each sub-component will collectively determine the overall terrorism risk profile. Terrorist strategies are dynamic rather than static. They develop new strategies that are adaptive to new environments. Applications of game theory are quite useful to analyze the terrorist strategies, new threats that may emerge and hence to determine the terrorism risk profile along US borders. Terrorism risk profile is represented by a joint probability function for fatalities and economic losses. This function should summarize the uncertainty about fatalities and economic losses suffered should the system fail as well as the uncertainty about the likelihood of a terrorist attack. The uncertainty about the consequences of a terrorist attack depends on the set of terrorism scenarios considered in making decisions. For instance, a dirty bomb attack is not likely to deliver very high number of casualties, whereas the consequences of a nuclear bomb attack are very likely to be catastrophic. Furthermore, economic consequences of a nuclear attack are potentially more devastating.

As defined earlier, failure of a sub-component is the success of terrorists to evade detection at US borders. The probability of failure is a function of the capital investments deployed, policies implemented to secure borders and the degree of terrorist sophistication. Failure of some of the sub-components will most likely lead to an immediate attack, whereas failure of others will not necessarily lead to success on the part of terrorists. In particular, if terrorists ship a dirty bomb with GPS surveillance, then the probability of success is almost one because they will most probably detonate the bomb before customs officials have any chance to inspect the container. However, a terrorist crossing between ports of entry without any apprehension may be captured later, before launching an attack.

Failure of some of the sub-components may be more critical than others. The criticality of a sub-component rests on significance of services it provides for national security, economic prosperity and public safety. The criticality of each sub-component can be quantified by the probability of a terrorist attack due to its failure multiplied by the expected disutility of damage upon attack that exploits failure of this sub-component. Alternative terrorism scenarios should be created to evaluate the expected disutility of damage. For instance, the set of alternative terrorism scenarios for attacks originating from a container will be different from the set of alternative scenarios for a security breach around critical maritime facilities.

The likelihood of a terrorist attack depends on many external factors as well as the level of deterrence at US borders and the likelihood of success. It also depends on the set of sub-components that fails. Some terrorist attacks may be result of a coordinated plan that exploits vulnerabilities on multiple sub-components. For example, failure of security between ports of entry to detect terrorists crossing the land borders may not immediately render a successful terrorist attack. In this case, the probability of success depends on the supply of explosives or weapons to terrorists which may not be readily available in the United States and thus should be smuggled through ports of entry. If the complexity of such a terrorist plot is increased with our efforts to improve security on multiple components simultaneously, then terrorists will probably have less incentive to attack.

The number of fatalities and economic losses in the case of a terrorist attack also depend on system's resilience and emergency response capability. The central decision maker should make decisions about how much resource to allocate to augment both capabilities. Most border security improvements will seek to decrease the probability of failure at a sub-component level. While this is a good strategy to mitigate risks, we have to recognize that the result of a terrorist attack may be far more catastrophic if we fail to implement a good emergency response strategy or resume normal operating conditions quickly. Improving emergency response capabilities shifts the probability from a high casualty consequence to a low casualty consequence. Hence border security decisions should not be made independent of emergency response resource allocation decisions.

The marginal value of an investment or a policy alternative is measured by the reduction of terrorism risk exposure after implementation of the alternative. Investments are assumed to have diminishing marginal value. Depending on risk tolerance of the central decision maker, risk reduction due to a particular investment may justify the extra cost. We recognize that terrorism risk exposure has multiple dimensions as terrorists are adaptive to new environments and risks are dynamic. Therefore, an investment may just result in shifting risks across sub-components. In this regard, bundling multiple investment alternatives may be the best strategy to fight terrorism effectively. One mistake would be to allocate all resources to a fraction of more critical sub-components and overlooking the threats posed at the other sub-components.

Intelligence is key to deploying resources to right locations. Intelligence will help make correct predictions about the possible terrorist behavior, hence develop strategies accordingly at the borders. It will also elicit probability of an attack, which will be used to determine the probability of failure at each sub-component. Terrorists may not have the immediate capability to launch all different forms of attacks, so intelligence will help characterize threats and also monitor terrorists' agenda. However, intelligence may not be fully reliable, and further may be noisy. Therefore, a balanced resource allocation across all the sub-components of the system is crucial.

III. MARITIME SECURITY

Maritime borders include 95,000 miles of coastline and 3.4 million square miles[3] of exclusive economic zone. Huge economic value of trade, number of jobs provided and multitude of stakeholders involved make security along coasts and waterways critical for the nation. In particular, port security is the underpinning of the US economy as a terrorist attack may deliver a serious blow to supply-chain operations, hence to continuity of business in the United States. Among the key facts that should be highlighted are:[4]

- 95% of overseas US trade by weight and 75% by value moves through US ports. Annually, more than 2 billion tons of domestic and international freight are transported on US waters.
- The US Department of Transportation forecasts that the volume of foreign trade moving through ports in 2020 will be at least twice as much as the 1996 level.
- Value of the US trade maintained an average growth rate of 10.2 percent between 1970-2003 whereas GDP growth was on the average 6.1 percent per year in the same period.
- In 2002, 4.9 million jobs were provided by exports of good and services offering 13-17 percent higher wages than the average US wages. 1.1 million of these jobs were at the ports.
- Share of international trade increased from 13 percent to 24 percent of GDP between 1970 and 2003. Port activities contributed $729 billion to nation's GDP. Transportation industry made $56 billion revenue out of port service operations whereas federal, state and local agencies were able to collect $16.1 billion of taxes.
- For recreational or traveling purposes, US waters host 134 million passengers on ferries, 78 million on pleasure boats and 5 million on cruise ships per year.
- Oil demand is satisfied by importing 3.3 billion barrels of oil per year transported across nation's maritime ports.

These figures provide more than adequate incentives for terrorists to use US waterways for an attack. Clearly, ports and other critical infrastructure along US coasts are open targets for those who wish to harm economic interests of the United States.

A. Threats in Maritime Domain

Terrorism threat from the maritime domain may come in three different forms: cargo, ship or illegal human traffic. Weapons or explosives may be concealed in containers, ships may be used as weapons to destroy critical infrastructure or terrorists may illegally cross the borders to launch attacks in the homeland. There is a continuum of maritime terrorism scenarios that essentially originate from a variant or combination of these three forms of threats. Clearly, threats in maritime domain have historically been realized for other non-terrorism purposes: piracy, illegal smuggling of contraband and illegal human traffic across the borders. Terrorists may use the expertise in other forms of maritime crimes that has accumulated over the years to exploit vulnerabilities in the system.

1. Piracy

Although historically not intertwined with terrorism, piracy is reemerging as a serious threat to impede conduct of global business. International community seems to turn a blind eye on the rise of piracy in open waters. However, in 2003, there were 445 attacks in which 21 crew members were killed, 71 reported missing and 359 were taken hostage[5]. The number of attacks dropped to 325 in 2004 with an increase in

[3] Source: Department of State website, www.state.gov

[4] Source: American Association of Port Authorities website, www.aapa-ports.org

[5] Annuals statistics released by International Maritime Bureau (IMB).

the death toll from 21 of previous year to 30. Actual figures may be far more disturbing. Shipping companies tend to underreport the incidents due to fears of increasing insurance premiums and lengthy investigations that may result in loss of reputation. As Singapore's Deputy Prime Minister Tony Tan recently said, "piracy is entering a new phase; recent attacks have been conducted with almost military precision. The perpetrators are well-trained, and have well laid out plans."[6] Annual cost of lost cargo has risen to $16 billion, mainly due to piracy, truck hijacking and theft around the ports.

Pirates have excelled in hijacking ships over the years. Once the ship is hijacked, "turning it into a phantom ship, erasing its original identity, is relatively easy"[7]. The ships are then known to be painted at remote docks and given a complete new identity. This is accomplished by getting a new registry by changing flags in "flag-of-convenience" countries[8]. The fleets of these countries are growing. Registration standards in these countries are relatively lax and there are no requirements on the nationality of crew members. Most "flag-of-convenience" ships are relatively unprotected against piracy. In 2003, 63% of all losses in absolute tonnage terms were accounted for by just 13 FOC registers.[9] These characteristics of flag-of-convenience ships render them and their cargo high risk.

There is minimal law enforcement at the international waters that pirates are known to be operating. Most piracy incidents take place in the Far East. Indonesia, Malacca Straits, Malaysia, Singapore Straits and South China Sea regions have witnessed most of the world's piracy attacks. Other geographical locations with reported cases include India, Philippines, Bangladesh, Gulf of Aden, Colombia, Venezuela, Vietnam, Red Sea and Dominican Republic.[10] Most of these countries have minimal resources for maritime patrolling and long coastlines, so pirates enjoy a huge degree of freedom in looting. Corruption among maritime officials also adds to the complexity of law enforcement in these waters. Modern pirates use technology for vessel surveillance, automatic weapons and motorized boats to hijack ships with valuable cargo. Combating piracy has become an enormously difficult task for maritime officials operating in these waters as pirates are well organized and armed.

As Table 4 illustrates, these waters are not foreign to terrorist groups. Modern day piracy offers loots that range from $8 million to $200 million per vessel.[11] This is a good financing opportunity for terrorist operations, so the inter-connection between piracy and terrorism is building up rather quickly. According to Indonesia's state intelligence agency, members of Jemaah Islamiyah have already admitted plans to attack ships passing through the Malacca Straits. Another terrorist group that has already been involved in hijacking incidents is Free Aceh Movement, a fundamentalist and separatist terrorist organization from Indonesia.

There is minimal cooperation between nations to combat piracy and each country is responsible to enforce law in their territorial waters. Pirates have a good understanding of their operational environment. They usually escape maritime officials by crossing sea boundaries and exploit vulnerabilities due to lack of

[6] Gal Luft and Anne Korin, "Terrorism Goes to Sea", Foreign Affairs, Nov/Dec 2004.

[7] John Burnett, "Dangerous Waters: Modern Piracy and Terror on the High Seas", New York: Penguin Group, 2002.

[8] A "flag-of-convenience" ship is defined as the ship that flies the flag of a country other than the country of ownership. International Transport Workers' Federation (ITF) maintains the list of "flag-of-convenience" countries. The current list includes the following nations: Antigua and Barbuda, Bahamas, Barbados, Belize, Bermuda, Bolivia, Burma, Cambodia, Cayman Islands, Comoros, Cyprus, Equatorial Guinea, French International Ship Register (FIS), German International Ship Register (GIS), Georgia, Gibraltar, Honduras, Jamaica, Lebanon, Liberia, Malta, Marshall Islands (USA), Mauritius, Mongolia, Netherlands Antilles, North Korea, Panama, Sao Tome and Principe, St. Vincent, Sri Lanka, Tonga and Vanuatu.

[9] ITF website: www.itfglobal.org

[10] "Worldwide Piracy Incidents Show a Decline", www.cargosecurityinternational.com.

[11] Ali M. Koknar, "Terror on the High Seas", Security Management, June 2004.

information sharing and international cooperation. The Malaysian Maritime Enforcement Center stated: “Under no circumstances would we intrude into each other's territory. If we chase a ship and it runs into the other side, we let the authorities there handle it”.[12] Therefore, penalizing maritime criminals is quite difficult and requires arrest authority unlimited by national boundaries.

2. Illegal Human and Contraband Traffic

Another concern is human and drug smuggling across maritime borders. This is particularly important because terrorists may use similar pathways to sneak illegal weapons through the border or to deliver a dirty bomb at the ports. Table 1 summarizes the statistics on the number of alien interdictions between 1995 and 2005. Most of the human smuggling operations are launched from Caribbean Waters although local governments in the region have been rather cooperative. Most Mexicans prefer the land route.

Containers have been used to conceal illegal aliens from China and Eastern Europe. The majority of illegal aliens seeking to enter the United States, either hiding in a freighter or a container are most usually discovered in miserable conditions. In 1999, 259 Chinese migrants aboard a freighter Wing Fung Lung have been intercepted while traveling with no bed or sanitation facilities.[13] In a relatively recent case, 32 Chinese nationals were found in two shipping containers at the Port of Los Angeles in January 2005.[14] Those traveling in containers may face death through starvation or asphyxiation. In 2001, Irish Police found a cargo container with 8 dead and 5 sick immigrants.[15] Similarly, in 2000 British Police have discovered 58 Chinese nationals in a truck that traveled to England on a ferry, suffocating at the brink of death. High risk of death does not seem to deter the aliens from seeking illegal entry into the United States for the prospects of economic prosperity. We need to assume that the resolve of terrorists for illegal entry is no less than that of illegal aliens.

Terrorists may use illegal human trafficking tactics to cross the American borders without bearing inhumane conditions as other economic migrants. In 2001, a stowaway was discovered at the port of Gioia Tauro in Italy traveling from Egypt to Canada.[16] Rizik Amid Farid of Egypt converted a container into a hotel room with a bed, a restroom, enough supplies of food, a laptop computer, two mobile phones and cameras. Among his belongings were a Canadian passport and airport security passes for Canada, which aroused the suspicion that he was involved in a terrorist plot to copycat 9/11 attacks. While this was never confirmed, the incident was a clear signal that a container stowaway scenario was far from being hypothetical. In 2004, the Israeli port of Ashdod was the location of a suicide bomb attack by two Palestinians who were able to conceal themselves in a container.[17]

Terrorists do not have to seek cooperation of ship owners or crew to plan and execute a container stowaway scenario. In many cases, stowaways board the ship without any recognition, and may actually attempt to hijack the ship.[18] The crew may not have effective means to confront stowaway problem once a

[12] Mark J. Valencia, “Conflation of Piracy and Terrorism in Southeast Asia: Rectitude and Utility”, Contemporary Southeast Asia, 01 August 2003.

[13] Diana L. Schneider, Robert Steiner, Joan Romaine, “Human Cargo: Health Conditions of Chinese migrants interdicted offshore by US authorities”, Journal of Community Health, February 2003.

[14] Eric Slater, “Human Smuggling Operation Probed”, Los Angeles Times, 17 January 2005.

[15] Brian Lavery, “Irish Police Find 8 People Dead and 5 Sick in Cargo Container”, New York Times, 9 December 2001.

[16] Dennis O'Brien, “Container Stowaway Raises New Fears Terrorist Suspect Tried to Cross Ocean in Steel Cargo Box”, The Virginian Pilot, 26 October 2001.

[17] Peter Enav, “Israeli Inquiry Finds Ashdod Bombers Used Hidden Container Compartment to Reach Port”, AP Worldstream, 30 March 2004.

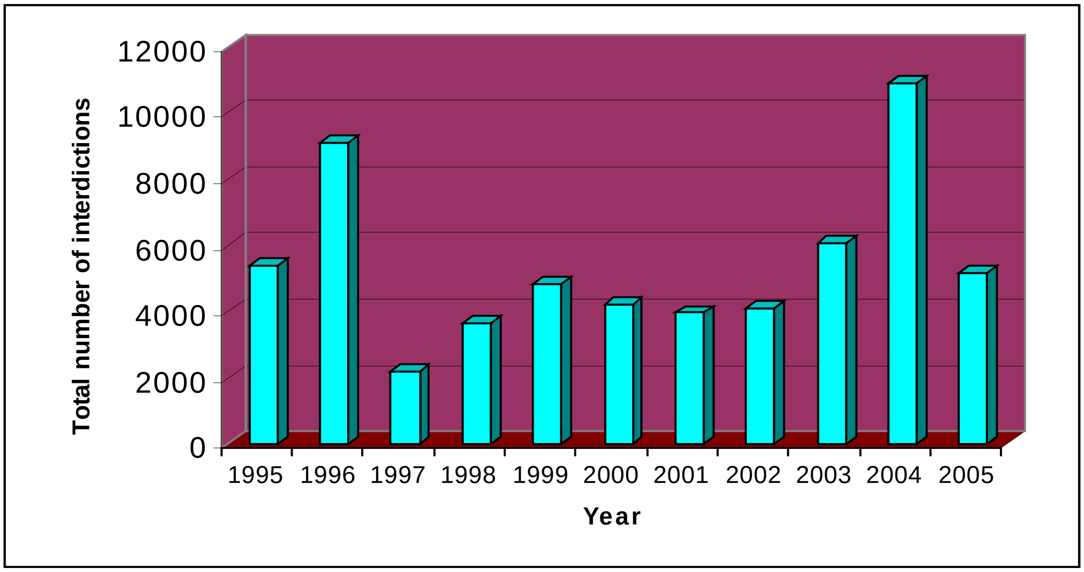
[18] Such a scenario was reportedly realized in 2000, when 14 Iranian stowaways hijacked an Italian ship. For more

stowaway is found on the ship. In some cases, stowaways are completely ignored to eliminate the possibility of armed confrontation. In other cases, stowaways are simply thrown overboard.[19] Most countries refuse to accept stowaways if they are citizens of another country. Hence, handing stowaways over to port officials may not be an alternative solution to the problem. The best solution from the perspective of ship crew seeking to minimize trouble on board could be simply ignoring the stowaway.

Table 1 Alien Interdictions along Maritime Borders as of May 2005[20]

Fiscal Year	Haiti	Dominic	Cuba	China	Mexico	Ecuador	Other
2005	1182	1950	1210	32	51	699	37
2004	3229	5014	1225	68	86	1189	88
2003	2013	1748	1555	15	0	703	34
2002	1486	177	666	80	32	1608	55
2001	1391	659	777	53	17	1020	31
2000	1113	499	1000	261	49	1244	44
1999	1039	583	1619	1092	171	298	24
1998	1369	1097	903	212	30	0	37
1997	288	1200	421	240	0	0	45
1996	2295	6273	411	61	0	2	38

Figure 2 Total Number of Alien Interdictions as of May 2005[21]



Smugglers introduce drugs and other illegal contraband either in small boats or in containerized cargo. It is widely believed that the multi-billion drug trade has historically exploited low inspection rates on containers

information, see “Iranian Stowaways Hijack Cargo Ship.”, United Press International, 12 June 2000.

[19] John Burnett, “Dangerous Waters: Modern Piracy and Terror on the High Seas”, New York: Penguin Group, 2002.

[20] Source: US Coast Guard Web Site: www.uscg.mil.

[21] Ibid.

at various ports. Detecting such illegal contraband has been likened to finding a needle in a haystack.[22] Table 3 lists some of the recent drug seizure incidents. Likewise, the Coast Guard has been facing the challenge to interdict drug traffic along shores for years. Drug interdiction statistics for the Coast Guard operations is provided in Table 2. Approximately, 75% of cocaine seizures took place in the Eastern Pacific[23] in recent years. Other regions with high traffic include the Gulf of Mexico, South Atlantic and Caribbean.

Table 2 The Coast Guard Drug Seizure Statistics by Fiscal Year[24]

Fiscal Year	Events	Vessels	Arrests	Marijuana (in pound terms)	Cocaine (in pound terms)	Cocaine's Imported Value, in Billion USD
2005	44	34	56	40,164.0	33,629.0	2.4
2004	104	71	326	25,915.0	242,435.0	7.7
2003	65	56	283	14,059.0	136,865.0	4.4
2002	58	40	207	40,316.0	117,780.0	3.5
2001	65	30	114	34,520.0	138,393.0	4.5
2000	92	56	204	50,463.0	132,480.0	4.4
1999	118	74	304	61,506.0	111,689.0	3.7
1998	129	75	297	31,390.0	82,623.0	3.0
1997	122	64	233	102,538.0	103,617.0	4.0
1996	36	41	112	42,063.0	44,462.0	1.1
1995	44	34	56	40,164.0	33,629.0	1.3
1994	67	28	73	33,895.0	47,333.0	1.8

Similar tactics may be employed by terrorists. There have not been any confirmed explosive or weapon smuggling cases in the United States through maritime borders using containerized cargo or small boats for terrorism purposes. However, in 2003, ABC News deliberately sent depleted uranium in a container from Indonesia and government screeners failed to detect the nuclear content. As Senator Dianne Feinstein (D-CA) stated, "…this is a case in point which established the soft underbelly of national security and homeland defense in the United States".[25] The container was loaded in Jakarta, Indonesia; a region relatively with a large population of radical terrorists and pirates. More recently, Armen Barseghyan of Armenia was charged in an alleged scheme to smuggle grenade launchers, shoulder-fired missiles and other Russian military weapons into the United States.[26] A more disturbing aspect of the case is its discovery by an FBI informant who posed as an al-Qaeda representative. This suggests that terrorists have no shortage of arms supply if they choose to attack the American homeland using smuggled weapons. Furthermore, we realize that the threat on commercial aviation by MANPADS or other shoulder-fired missiles should not be ignored.

[22] An Australian Customs Official has been reported to make that comment. "$18 million Drug Seizure Like Needle in a Haystack", AAP General News Wire, 22 April, 2005.
[23] United States Coast Guard Fiscal Year 2004 Report.
[24] Source: US Coast Guard Web Site: www.uscg.mil
[25] "How Secure are US Borders?", ABC News, www.abcnews.com, 11 September 2003.
[26] "Suspect in Weapons Smuggling Case Extradited to United States", AP Worldstream, 18 April 2005.

Table 3 Selected Drug Smuggling Incidents in a Container

Port	Year	Event Description
San Francisco	1991	In one incident 1080 pounds of heroin was seized in a cargo container. The shipment originated from Myanmar, Laos and Thailand. It was the biggest heroin seizure in the United States at the time.[27] The value of shipment was estimated to be between $2.7 billion to $4 billion.
Newark	1998	Customs agents seized 1300 pounds of cocaine in a container full of rolls of wrapping paper. The shipment originated from a paper mill in Santos, Brazil. The estimated value was approximately $40 million.[28]
Miami	1999	7,086 pounds of marijuana was found hidden in 40-foot refrigerated container load of yams. The origin of shipment was Kingston, Jamaica.[29]
Houston	1999	1500 pounds of cocaine shipment was discovered inside bags of frozen fruit pulp in a refrigerated container. The ship arrived from Venezuela.[30]
Miami	2002	Customs agents found 3,618 pounds of cocaine in a scrap paper shipment from Dominican Republic. The value of the shipment is estimated to be $32 million.[31]

3. Maritime Terrorism

While terrorists have historically focused on land targets, there is no shortage of terrorism events in national and international waters. Table 4 demonstrates that terrorists have exploited vulnerabilities in global maritime operations and launched successful attacks to accomplish their political and economic goals. International waters have long been penetrated by terrorists and there is virtually no protection for commercial ships against this growing threat. US vessels are not immune from the rise of maritime terrorism as shown by the boat attack on naval destroyer Cole in 2000. It is even more disturbing to realize that terrorists can sabotage the flow of international trade with relatively less effort than in 9/11. They have a continuum of options. For instance, they may choose to ship a container with a nuclear or radiological bomb or attack tankers to disrupt energy exports. Hence, there is clearly a need to develop a systematic approach to mitigate catastrophic risks that the nation is exposed from its shores. As terrorists develop their maritime terrorism skills, the probability of delivering an attack with catastrophic consequences on US economic interests will increase. Al-Qaeda has already stated interest to this end. After the attack on French tanker Limburg 2002, Osama Bin Laden released an audio tape that stated “By God, the youths of God are preparing for you things that would fill your hearts with terror and target your economic lifeline until you stop your oppression and aggression.”[32] Al-Qaeda, Jemaah Islamiyah and other terrorist organizations can utilize their skills and resources that they have historically revealed to launch attacks on critical coastal targets in the United States, to tamper with US-bound cargo to deliver illegal weapons, and explosives, or to develop radiological bombs which will later be destined to US ports.

[27] Joseph Treaster, “US Officials Seize Huge Heroin Cache”, New York Times, 22 June 1991.
[28] Ronald Smothers, “Customs Agents Seize 1,300 pounds of Cocaine”, New York Times, 11 June 1998.
[29] Dan Morain, Philip Hager, “Customs Suspects Drug-smuggling Conspiracy”, Journal of Commerce, 10 November 1999.
[30] Kevin Hall, “Security is a Growing Concern at Nation’s Container Ports”, Journal of Commerce, 27 September 1999.
[31] Thomas Kielbasa, “Guard Counter-drug Ventures Pay Off Big in 24-hour Period”, National Guard, September 2002.
[32] “Tape Warns of More Attacks against United States.”, USA Today, 7 October 2002.

Table 4 Recent History of Maritime Terrorism[33]

Year	Event
1961	Opponents of Antonio de Oliviera hijacked Portuguese passenger ship Santa Maria and later were provided political asylum in Brazil.
1963	Venezuela's communist insurgent group, the FALN, hijacked the Venezuelan freighter SS Anzoategui. The search activities were unsuccessful as the terrorists entered the Brazilian port of Belem and received political asylum.
1970	The US-flag freighter Columbia Eagle was seized by two crew members protesting the war in Vietnam, while on a voyage to Thailand with a cargo of ordnance. Both mutineers were given asylum in Cambodia. One later returned to stand trial for mutiny and assault whereas the second has never been heard from again.
1971	Palestinian fighters attacked a Liberian tanker Coral Sea to deter usage of Israeli port of Eilat on the Red Sea.
1971	Members of the Armed Revolutionary Action carried an attack on the Portuguese ship off Mozambique coast, killing 23 crew members.
1971	IRA attempted to blow up cruise liner Queen Elizabeth II.
1972	Soviet research ship was bombed by Castro opponent group JCN in Key Biscayne, Florida.
1973	A Palestinian group, Black September, sank the Greek charter ship "Sanya" carrying 250 US tourists on board and heading to Haifa, Israel. No casualties were suffered.
1973	Cuban nationalists bombed a vessel awaiting cargo at a Miami river dock to protest government of the Bahamas for the murder of Cuban nationals.
1974	Cuban nationalists dropped a hand grenade onto Soviet cruise vessel Maxim Gorki. Two crew members were injured.
1974	Two Japanese Red Army and two Palestinian PFLP members hijacked a passenger ferry, Laju, in Singapore. They were given a safe passage by the Singapore government.
1974	A Greek freighter, Vory, was hijacked by the members of a group called Moslem International Guerrillas in Karachi.
1974	Jewish Defense League sank a ferry in Los Angeles Harbor named Caribe Star.
1975	Filipino separatist group MNLF hijacked a Japanese freighter with 27 persons aboard in Manila.The terrorists surrendered unconditionally and released all the hostages.
1975	A Chilean training vessel and a Kobe University ship docked at the International Ocean Exposition in Okinawa were attacked by terrorists using Molotov cocktails. Two sailors were injured.
1975	Argentine opposition movement Monteneros carried a well-orchestrated attack on the navy ship 3,500-ton Santisima Trinidad. The explosion damaged all the electronics aboard and delayed the deployment by a year.
1976	Cuban nationalists carried out four different attacks, two of which were in US waters, mainly targeting Soviet and Cuban vessels.
1976	Four Greek vessels were sunk by limpet mines placed by frogmen in Lebanon. The attacks were believed to be the members of a Lebanese Christian Group.
1977	Polisario Front guerillas attacked a Spanish trawler with mortar and machine-gun fire seized three Spanish firemen.
1979	Lord Mountbatten's fishing yacht was exploded by an IRA bomb in Mullaghmore, Ireland, killing four people including the lord himself.

[33] Source: Terrorism Knowledge Database, www.tkb.org and Krzysztof Kubiak, “Terrorism is the New Enemy at Sea”, United States Naval Institute Proceedings, December 2003

Table 4 continued

Year	Event
1980	Maltese Liberation Front attacked a Libyan gunboat in the port of Genoa, Italy. The bomb was thought to be placed by frogmen.
1980	Polisario Front guerillas carried out three attacks, one on a Maroccan, one on a Portugese and the other on a Spanish vessel.
1981	An Iranian nationalist paramilitary organization seized the rocket boat Tabarzin to protest Khomeini.
1981	Polisario Front attacked a Portuguese fishing vessel off the coast of Western Sahara.
1982	A Lebanese cargo ship was blown up at the port of Tyre, Lebanon.
1983	IRA blew up a British cargo vessel in Lough Foyle.
1983	A nationalist Argentine group attacked a Danish ship in Falkland Islands. The ship was carrying construction material which would be used to build a monument for the British soldiers died in military conflict between Argentina and Great Britain the year before.
1984	Nicaraguan Democratic Force and the Democratic Revolutionary Alliance sank or damaged 11 ships by laying mines around the entry of the main ports in the country.
1984	UNITA, a terrorist group fighting against the government of Angola, executed a mine attack on two freighters in the harbor of Luanda.
1984	Hezbollah executed multiple attacks on ships passing through Suez Canal laying mines to the southern entrance of the canal. 19 ships were affected from this organized attack. It was later claimed that 190 acoustic mines were laid in the canal. Libya was thought to be involved in the attacks.
1985	Polisario Front were held responsible from multiple attacks held off the coast of Morocco
1985	Italian cruise liner Achille Lauro was hijacked off the Egyptian coast by the Palestinian Liberation Front with 511 passengers on board to demand the release of 50 Palestinian prisoners in Israel. One American passenger was killed. The terrorists were later captured in Italy after surrendering the ship to Egyptian officials with the guarantee of safe passage out of Egypt.
1985	A Cypriot vessel hits a mine which was laid in the Red Sea by Hezbollah.
1985	Al-Fatah captured an Israeli yacht in Cyprus to demand the release of 20 prisoners. 3 Israelis claimed to to be Israeli spies were killed by the terrorists before surrendering to the police. Israel, in retaliation, attacked Tunisia.
1986	Polisario Front carried out three separate attacks on Spanish and Soviet ships off the Maroccan coast.
1987	Abu Nidal captured a French yacht off the coast of Gaza Strip to warn Arab leaders not to entitle King Hussein of Jordan to be the representative of Palestinians in peace talks. At the request of Qaddafi, all the hostages were released.
1988	Abu Nidal attacked a Greek cruise ship, killing 11.
1988	As a result of guerrilla ambush, two people were killed on a ferryboat with an American delegation on board.
1990	A gunboat attacked a Cypriot ship killing 1, injuring 25.
1990	Eritrean separatists attacked and sank a Polish freighter Boleslaw Krzywousty from the Eritrean shore (then-Ethiopian shore) by rocket fire.
1990	Supply ship for Victoria was attacked by IRA.
1991	Somalian nationalists hijacked a Polish cargo ship in the gulf of Aden.

Table 4 continued

Year	Event
1996	Avrasya, a ferry sailing from Trabzon, northern port of Turkey, to Russia was hijacked by Chechen separatists demanding the withdrawal of Russian troops from a Daghestani village. The separatists were later captured at a Turkish port, Eregli, after a series of negotiations. No casualties were suffered.
1997	Two armed attacks by Tamil Tigers against Chinese and North Korean ships.
2000	Al-Qaeda attacked the US destroyer Cole while refueling in Yemen, port of Aden, by exploding a small boat nearby the vessel.
2001	Suicide attackers of Tamil Tigers attacked a ship carrying fuel. Five boats full of explosives were involved in the attack.
2002	As a result of a suicide boat attack, French tanker Limburg was damaged, killing one, injuring twelve. A radical islamic group claimed the attack, stating that they were targeting a US Navy vessel instead.
2003	A Turkish tanker carrying oil from Turkey to Iraq was attacked.
2003	It is claimed that a suicide attack on an Israeli ship at the port of Antalya in Turkey was not launched because the ship could not dock due to weather conditions. The terrorist then committed a suicide attack ramming truck full of explosives into British Consulate General in Istanbul, Turkey.
2004	A bomb exploded at the Pakistani port of Karachi, killing two.
2004	A series of bombs exploded to discourage workers' involvement in a port project.

Further intelligence seems to confirm that Al-Qaeda may still be planning attacks on maritime targets. In 2002, Al-Qaeda's former chief of naval operations was said to confess plans to attack ships passing through the Strait of Gibraltar.[34] The scheme was later foiled by Moroccan officials. The alleged mastermind of the terrorist attacks on 9/11, Khalid Shaikh Mohammed, was reportedly involved in a plot to export weapons and explosives into the United States.[35] To this end, he was reported to make an offer to an import/export firm to use their containers for shipping the illegal contraband to New York/ New Jersey port. Drug dealers are known to employ a similar tactic of buying out a trustworthy shipping company to disguise their shipments for years.[36] Drug smuggling chains can be discovered after observing patterns of shipments. However, maritime security officials have no luxury to observe such patterns to counter terrorism threat because one successful attempt to evade detection at the ports may render catastrophic consequences.

The threat of maritime terrorism is real and we should be aware of the vulnerabilities in the system to effectively confront potential evil doers. Potential gaps in border security probably incentivize those who wish to harm the United States. We discuss the vulnerabilities in the next section.

B. Vulnerabilities along Maritime Borders and Countermeasures for Risk Mitigation

Maritime Security will be discussed under two main categories: port security and security in US waters. Maritime Transportation Security Act (MTSA) signed by the President Bush on November 25, 2002, was designed to address the security of ports and waterways. As a result of this act, maritime security

[34] "A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction", Address by Michael Richardson on September 2004 to the Victorian Branch of the Australian Institute of International Affairs. Michael Richardson is currently a visiting senior research fellow at the Institute of South East Studies in Singapore.

[35] Daniel Klaidman and Mark Hosenball, "Terrorism: Ties to a Qaeda Chief.", Newsweek, 18 August 2003.

[36] CRS Report to Congress, "Port and Maritime Security: Background and Issues for Congress", 27 May 2005.

enforcement responsibility has been mainly assigned to the United States Coast Guard (USCG), the Bureau of Customs and Border Protection (CBP) and Transportation Security Administration (TSA) under Department of Homeland Security (DHS) as well as Maritime Administration (MARAD) under Department of Transportation (DOT). Ports also have responsibility to police the port area. The USCG has the lead responsibility in most of the MTSA assignments as well as the security of US waters and coastal targets. On the other hand, CBP assumes a key role in improving security of inbound cargo at maritime ports.

1. Port Security

The efforts to counter domestic terrorism have significantly shifted towards ensuring security of aviation industry after the blatant attacks on WTC. However, as our antiterrorist thinking evolved, we have realized that a more comprehensive approach to homeland security is required. Ports rank relatively higher in the homeland security agenda as the potential impact of hampering port operations could be an economic disaster. Since 9/11, ports have been awarded a total of $565 million for security upgrades.[37] According to a Brookings Institution's report, a port shutdown could cost the economy as high as $1 trillion.[38] However, port security has been increasingly intertwined with the security of containerized cargo in the public and media. While containers are inarguably the "Trojan Horses" of the modern era, failure to recognize the other vulnerabilities may leave the US homeland unguarded for another surprise attack.

Following characteristics of maritime ports make them a potential target for terrorists,[39]

- Ports encompass a large operational area that is hard to secure either from water or land.
- Volume of trade that crosses through nation's ports is huge, making it practically impossible to check the contents of each piece of cargo while ensuring efficient and timely delivery of goods to their final destinations.
- Many critical coastal targets such as petroleum tank farms, hazardous material storage facilities, bridges and factories are located around the ports.
- A successful attack is likely to result in high number deaths as major US cities are located near waterways.
- Number of stakeholders is high, with usually conflicting priorities. This undermines the effectiveness of security measures.
- Ports employ a good number of people, all facing the risk of injury or death in the case of an attack. Furthermore, transportation facilities with high concentration of passengers are located near ports.

Federal government urged the Coast Guard to conduct risk assessments of 55 major ports in 2002. The assessments are already finished. However, according to GAO[40], the progress made in these assessments is not satisfactory as it lacked a management strategy and an implementation schedule. Furthermore, GAO argues that the Coast Guard developed a system that overlooks some of the security gaps around the ports. The Coast Guard plans to address the problem by introducing a geographic information system (GIS) that will provide information required to develop contingency plans and effective countermeasures against specific threats and scenarios. If intelligence on a possible attack is received, a well-designed GIS should be able to identify the critical facilities in the geographical area and inform the user about the availability of resources to monitor and respond to the threat. Examples of critical facilities include bridges, power

[37] Elana Schor, "Port Security a Major Concern on the Gulf Coast", The Sun Herald, 20 March 2005.

[38] O'Hanlon, Michael et al., "Protecting the American Homeland: A Preliminary Analysis", The Brookings Institution, 2002.

[39] GAO Testimony GAO-02-993T provides a good discussion on the vulnerabilities around the maritime ports.

[40] GAO Testimony GAO-05-364T, "Coast Guard: Observations on Agency Priorities in Fiscal Year 2006 Budget Request", 17 March 2005.

stations, warehouses and nuclear or chemical power plants. Furthermore, a well-designed GIS is necessary for performing a comparative risk assessment of facilities to support emergency response decisions. For instance, if there is credible intelligence that bridges around a port is subject to an emerging waterborne threat, then an ideal GIS tool should give accessibility information on each bridge to determine which one of the bridges is a more likely target. GAO[41] believes that the functional requirements of this system have not been identified. Without building a system that will help effectively respond to external threats, the fault tolerance and the resilience of the entire port operations will be low.

Under port security, there are four sub-components of the border security system: cargo security, access to secure areas, cruise lines and security around the port perimeters. Most of the discussion centers around the cargo security as the terrorism risk is maximal in monitoring the contents of cargo without interrupting the flow of trade.

a. Cargo Security

The companies are facing the dilemma of achieving efficiency and security in containerized cargo transportation simultaneously. Willis and Ortiz[42] describe the capability of meeting these goals by evaluating five measurable supply chain performance criteria:

- *Efficiency* is the quick and cheap delivery of goods. This is particularly important in a competitive business environment as most companies can offer low prices by reducing their transportation costs and satisfy their customers by short order lead times. If a company fails to implement a good supply-chain management strategy, then the chance of survival is rather dim, if not impossible.
- *Shipment Reliability* refers to the capability of avoiding shocks such as thefts, and accidents in the supply-chain network.
- *Shipment Transparency* is the ability to accurately present the contents of the shipment to authorities when information is needed. The companies should keep track of their shipments to enhance their transparency. This will mitigate the negative impacts of supply-chain delays and shocks as the countermeasures will be taken earlier.
- *Fault Tolerance* is responding effectively to disruptions retaining maximum operational capability possible. If minor failures or external threats have the potential to restrain and stop most of the system functions, then the vulnerability is high.
- *Resilience* is the capability of returning to normal operations quickly should the system become unable to operate. Long delays may lead to severe economic consequences.

We analyze cargo under two headings: containerized and general cargo. Most of the discussion will be centered on containerized cargo as the bulk of international trade flows in containers.

I. Vulnerabilities in Containerized Cargo Security

There exist various forms of security gaps in cargo movement between points of origin and destination. These gaps are relatively more alarming as we have to seek cooperation of other nations to address them. There are multiple phases in transportation of cargo across the supply-chain: loading at the warehouse, land transportation, warehousing and loading at the port of origin, sea transportation and unloading at the port of destination.

[41] GAO Report, GAO-04-1062, "Better Planning Needed to Help Ensure an Effective Port Security Assessment Program", September 2004.
[42] Willis, Henry H., Ortiz, David S., "Evaluating the Security of the Global Containerized Supply-Chain", RAND Technical Report, 2004.

i. Loading Phase at the Warehouse

Terrorists may load illegal weapons and explosives at the warehouse or distribution center from which the cargo is dispatched. To this end, they may either cooperate with workers involved in the loading phase, or tamper with the cargo without notice. In other words, terrorists may exploit vulnerabilities, some of which are listed below, at the loading facility and ship deadly cargo:

- Gaps in physical security around the facility. These could be in multiple forms: unlocked doors and gates, insufficient monitoring in and around the warehouse, easily penetrable fences, lack of guardians protecting the facility...etc.
- Insufficient background checks of workers.
- Lax procedures for visitor admission.
- Insufficient training of workers to detect and respond to anomalies at the facility.
- Improper storage of empty containers.

ii. Land Transportation Phase.

This is a relatively critical phase in that there are multiple stakeholders that would benefit from improved intermodal land transportation security. This phase starts with the dispatch of the container from the originating warehouse and ends at the port of origin. Cargo theft during this phase of the transportation is a huge problem that the companies need to confront in the modern era. For instance, cargo insurers in industrialized nations like Italy, Australia, Germany and France, with which the United States has extensive overseas trade ties, face enormous claims from cargo theft every year.[43] More recent statistics suggest that cargo theft is on the rise in Belgium, Netherlands, France and United Kingdom.[44] In particular, high value cargo that includes pharmaceuticals, luxury clothing, electronics and computer hardware are also high risk.

During this phase, cargo moves in one of the two modes of transportation: truck or rail. However, due to economies of scale, the mode of transportation may not remain the same during travel to the port. Cargo may be transferred from one mode to another (intermodal transfer), or simply within the same mode (intramodal transfer). Some of the potential vulnerabilities in this phase are as follows:

- Security breaches at the transfer points. Cargo may wait temporarily for some time at the transfer facility. If the facility is poorly guarded, this gives a good opportunity to tamper with cargo.
- Insufficient background checks on the truck and locomotive drivers.
- Frequent stops in transit. For instance, due to daily work hours limitation, the truck may make stops before reaching destination, and this increases the chance of cargo theft and tampering.
- Funding challenges. Since there are many stakeholders, determining the funding source for security enhancements is a challenge.
- Tremendous variety of freight hauled on railroads and highways. This adds extra complexity on the regulatory environment.

iii. Port of Origin

After a land transportation phase, cargo reaches the port of origin. The cargo may be stored around the port

[43] Lee Coppack, "Hijackings Haunt Cargo Underwriters", National Underwriter Property & Casualty-Risk & Benefits Management, 11 October 1993.

[44] "September Freight Crime Bulletin from EUROWATCH", www.cargosecurityinternational.com, 10 October 2005. Other reports published by EUROWATCH earlier in 2005 suggest a similar trend in Spain, Russia, Ireland and Italy.

perimeter before loading on the ship. After clearance, cargo is loaded and shipped to the point of destination. Among the potential vulnerabilities in this phase are:

- Security breaches around port perimeters. The container may be stored at warehouses before the procedures for import are completed.
- Insufficient background checks for port officials. In some countries, corruption is a problem at customs. Thus, there is a risk of terrorist collaboration with port officials.
- Lack of state-of-the-art inspection equipment. Ports may not have incentives to inspect outbound cargo. This will reduce the likelihood of detection.
- Unauthorized access to the secure areas in the port.
- Lack of procedures to protect against unmanifested material being introduced aboard.
- Insufficient training of port workers/officials to detect anomalies and respond accordingly.
- Security breaches in storing and shipping empty containers.

iv. Sea Transportation

In this phase, cargo moves on a ship that may visit other ports before arriving at a US port. The integrity of cargo may be compromised due to following list of potential vulnerabilities:

- Lack of security guidelines to combat piracy/stowaway threat.
- Insufficient background checks on the ship crew.
- Security breaches at the ports visited en route.

v. Port of Destination

Cargo finally arrives at a US port. It may then be hauled by a truck or by rail to the final inland destination. Potential vulnerabilities at US ports are similar to that of port of origin. One difference is that the threat may come from homeland. For instance, cargo may be tampered with during storage phase around the port perimeter. However, this is a relatively unlikely scenario. If there are terrorists already in the United States who plan to transport weapons or explosives to other destinations within the country, then they would probably do so by trucks. While one may compile a long list of vulnerabilities at US ports of entry, relatively few of them would challenge integrity of cargo present at the port as there are relatively easier avenues to transport weapons or explosives in the country.

II. Countermeasures and Policies to Address Vulnerabilities in Containerized Cargo Trade

The federal government unveiled new initiatives to address the problem of container security after 9/11. By implementing Container Security Initiative (CSI), Customs-Trade Partnership against Terrorism (C-TPAT), Megaports Initiative and Operation Safe Commerce (OSC), the government seeks to incentivize stakeholders involved in maritime operations and foreign governments to consider countermeasures that improve security in transit. Without proper incentives, improvements in security appear merely as extra cost and burden on other parties involved in homeland security effort. For instance, in the case of interdependent security, companies won’t invest in security improvements at all if all the other parties are believed to do so.[45] Consequently, risks will not be mitigated due to underinvestment in countermeasures.

[45] Heal, G. and Kunreuther, H., "You Only Die Once: Managing Discrete Interdependent Risks.", Working Paper 9885, National Bureau of Economic Research, Cambridge, MA. June, 2003.

i. Container Security Initiative (CSI)

CSI is an effort to extend US borders to confront external threats outside the homeland. It was announced in 2002 by the CBP commissioner Robert C. Bonner. The main objective is to identify and pre-screen the containers that pose risks of terrorism at the port of origin as well as to promote development of smart containers that external parties cannot tamper with. By implementing the initiative, CBP seeks to reduce the inspections at US ports, thereby ensuring efficient flow of trade. 40 operational ports in Europe, Africa, Asia and Americas participate in this initiative. These ports are listed in Table 5.

The criteria for expansion to new foreign ports are based on trade volume, location and strategic importance. Eligibility of a foreign port into this program requires installation of non-intrusive inspection (NII) equipment and deployment of trained customs officials who can perform inspections. US Customs officials visit participating ports under the initiative to target and pre-screen the containerized cargo. They also visit the loading facilities to check the security standards. To this end, CBP assembles a CSI team with members from either CBP or ICE. It is expected that participating foreign ports are willing to share critical information with the CBP officials to help targeting of high risk cargo. CBP recognizes that advance information is key to security operations. In order address this issue, “24-Hour Rule” was initiated. The rule requires the carriers to report their cargo manifests 24 hours before the cargo leaves the port of origin. This provides the time frame for risk assessment of cargo.

Table 5 Ports Currently under CSI[46]

Americas		**Asia**		**Europe**	
Port	**Country**	**Port**	**Country**	**Port**	**Country**
Montreal	Canada	Tanjung Pelepas	Malaysia	La Spezia	Italy
Vancouver	Canada	Port Klang	Malaysia	Genoa	Italy
Halifax	Canada	Colombo	Sri Lanka	Naples	Italy
Santos	Brazil	Kaohsiung	Taiwan	Gioia Tauro	Italy
Buenos Aires	Argentina	Laem Chabang	Thailand	Livorno	Italy
Asia		Dubai	UAE	Felixstowe	United Kingdom
Port	**Country**	**Europe**		Liverpool	United Kingdom
Singapore	Singapore	**Port**	**Country**	Thamesport	United Kingdom
Yokohama	Japan	Rotterdam	The Netherlands	Tilbury	United Kingdom
Tokyo	Japan	Bremerhaven	Germany	Southampton	United Kingdom
Nagoya	Japan	Hamburg	Germany	Pireaus	Greece
Kobe	Japan	Antwerp	Belgium	Algeciras	Spain
Hong Kong	China	Zeebrugge	Belgium	**Africa**	
Shanghai	China	Le Havre	France	**Port**	**Country**
Shenzhen	China	Marseille	France	Durban	South Africa
Pusan	South Korea	Gothenburg	Sweden		

Real-time information sharing between customs officials is one of the advantages of implementing CSI. Automated Targeting System (ATS) is used to help select the high risk cargo. This system uses cargo manifest information, targeting rules, shipper and customer/importer information to assign each container in a risk category (i.e., low, medium, high). Intelligence reports and research assistance provided by National Targeting Center (NTC) are also checked to make the final decision regarding inspection of a specific

[46] Source: www.cbp.gov.

container. The containers with high risk score are to be inspected. The medium risk containers are subject to further research. Inspections are performed by local officials. However, CSI team is given the option to monitor inspections. Figure 3 summarizes the targeting and inspection procedures at domestic ports.

Figure 3 CBP's Domestic Process for Targeting and Inspecting Cargo Containers[47]

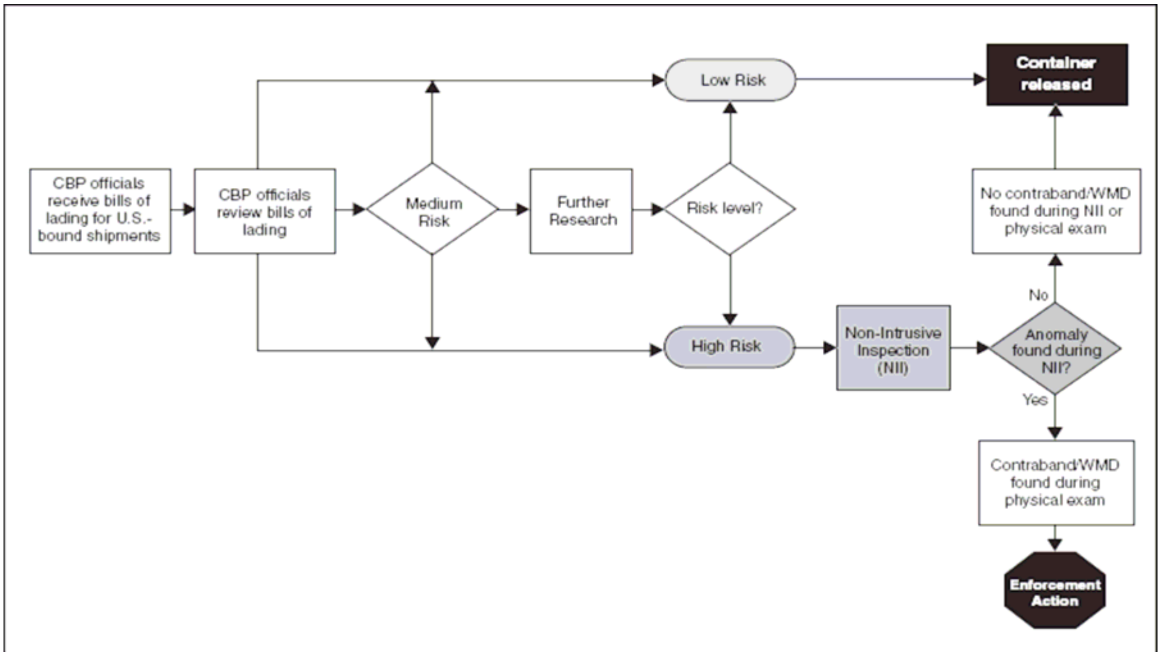
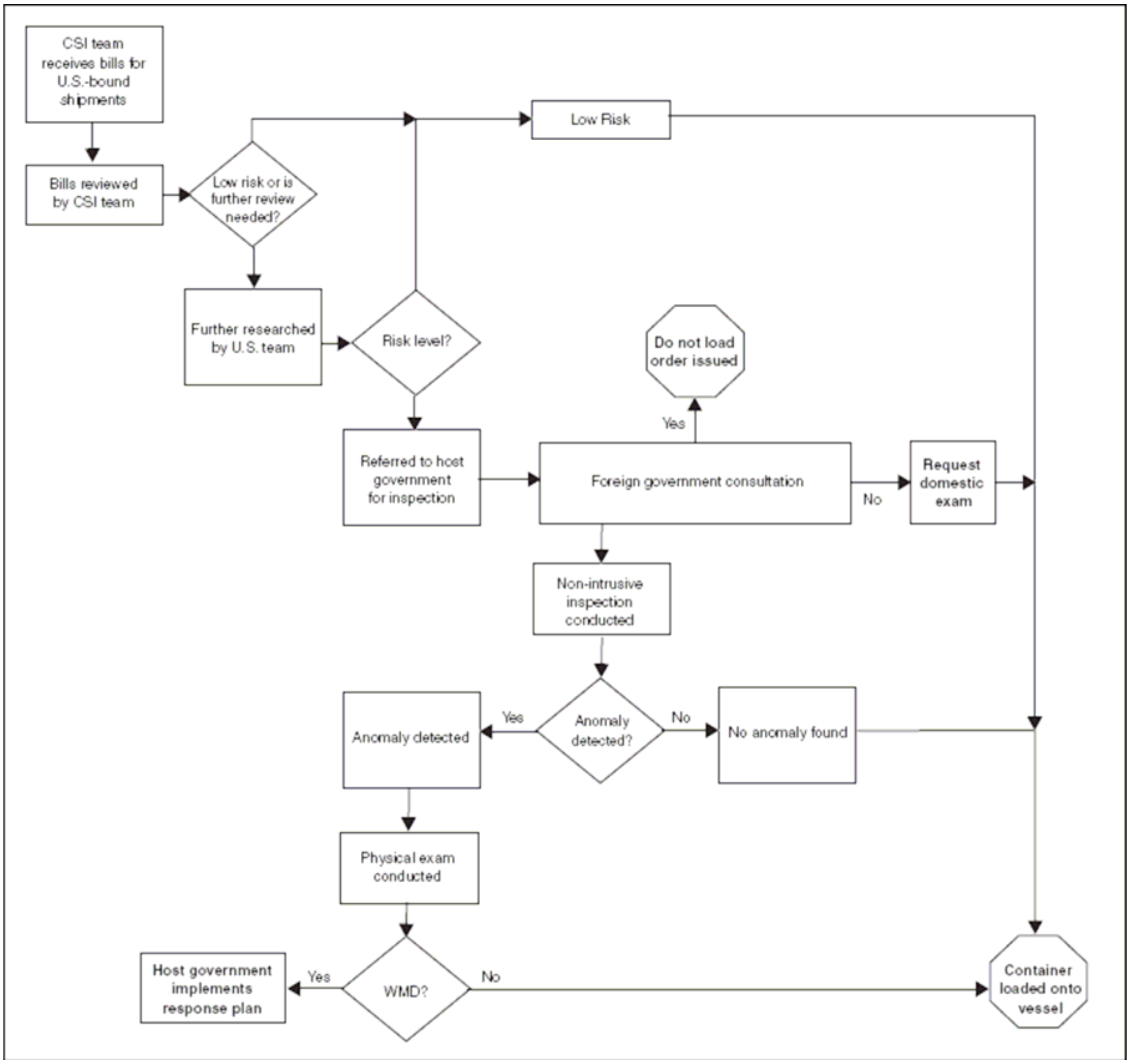

CBP officials receive bills of lading for U.S.-bound shipments
CBP officials review bills of lading
Medium Risk
Further Research
Risk level?
Low Risk
Container released
High Risk
Non-Intrusive Inspection (NII)
Anomaly found during NII?
No
Yes
No contraband/WMD found during NII or physical exam
Contraband/WMD found during physical exam
Enforcement Action

Table 6 Top 10 Foreign Ports, by Number of US-bound Containers, 2001[48]

Foreign Ports	Number of US-Bound Containers	Percentage of total containerized US-Bound Cargo, by volume
Hong Kong, China	558,600	9.8
Shanghai, China	330,600	5.8
Singapore	330,600	5.8
Kaohsiung, Taiwan	319,200	5.6
Rotterdam, The Netherlands	290,700	5.1
Pusan, South Korea	285,000	5
Bremerhaven, Germany	256,500	4.5
Tokyo, Japan	159,600	2.8
Genoa, Italy	119,700	2.1
Yantian, China	114,000	2
Total	2,764,500	48.5

[47] Source: GAO Report, GAO-05-557, "Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts", April 2005.
[48] Source: GAO Report, GAO-03-770, "Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors", July 2003.

Figure 4 CSI Process for Targeting and Inspecting Cargo Containers Overseas[49]


CSI team receives bills for U.S.-bound shipments
Bills reviewed by CSI team
Low risk or is further review needed?
Low Risk
Further researched by U.S. team
Risk level?
Do not load order issued
Yes
Referred to host government for inspection
Foreign government consultation
No
Request domestic exam
Non-intrusive inspection conducted
Anomaly detected
Yes
Anomaly detected?
No
No anomaly found
Physical exam conducted
Host government implements response plan
Yes
WMD?
No
Container loaded onto vessel

Should the officials choose to inspect the cargo, a gamma-ray or X-ray shot of the container is taken using the Vehicle and Cargo Inspection System (VACIS) to perform visual detection. Inspectors may decide to open the container and conduct physical inspections in case they detect anomalies. The decision of physical inspection is technically given by both CBP and local officials. CBP states that their goal is to inspect %100 of the high risk cargo. For nuclear content, radiation detection devices such as radiation portal monitors are used. The inspection process as described here may slow down the container flow through seaports. In order to attract foreign seaports into the initiative, both parties agree that CSI port shipments will be given the priority in processing in the case of a terrorist attack that halts port operations. Likewise, US port authorities may choose to limit their operations to CSI ports in the case of a minor attack. Accordingly, shipments that originate from non-CSI ports may experience long delays if a terrorist attack triggers full or partial shutdown of maritime ports. Most companies will factor potential port delays in their choice port of origin for their shipment. As ports compete to increase their share in the global supply-chain network, they may be willing to join the list of ports that ship low risk cargo to the United States.

[49] See Footnote 47.

Table 7 Top 10 Domestic Ports, by Number of US-bound Containers, 2001[50]

US Ports	Number of US-Bound Containers	Percentage of total containerized US-Bound Cargo, by volume
Los Angeles	1,774,000	24.7
Long Beach	1,371,000	19.1
New York - New Jersey	1,044,000	14.6
Charleston	376,000	5.2
Savannah	312,000	4.3
Norfolk	306,000	4.3
Seattle	284,000	4
Tacoma	273,000	3.8
Oakland	268,000	3.7
Houston	233,000	3.3
Total	6,241,000	87

ii. Customs-Trade Partnership against Terrorism (C-TPAT)

C-TPAT is a voluntary program of partnership between the public organizations and private companies to improve supply-chain security. It was announced in November 2001 and received a warm welcome from most of the major trading companies. As of April 2005, approximately 9100 companies are registered to the program. Participating companies are asked to perform self-assessments of their whole supply-chain and to develop shipping guidelines for their suppliers. The government seeks to employ the private sector's leverage on their global suppliers to address one of the most vulnerable phases of container shipment: loading phase. The US government has no control on foreign companies to follow proper guidelines in loading and transporting goods to the United States. However, companies can use their buying power to have their downstream suppliers enforce relevant security measures.

Private sector enjoys reduced and expedited inspections under this program as their cargo are "low-risk". Companies are also encouraged to use smart containers as their standard medium of trade. A potential benefit of smart containers will be to eliminate the routine inspections. Reduced delays for shipments are vital for companies who are already operating under tight operating margins. After 9/11 Ford shut down five of its US plants due to engine and drive-train parts shortage.[51] Toyota and General Motors also came to the brink of production halt at some of their major plants. Companies seek to avoid such severe consequences in the case of an attack to get priority treatment from the federal agencies to process their shipments.

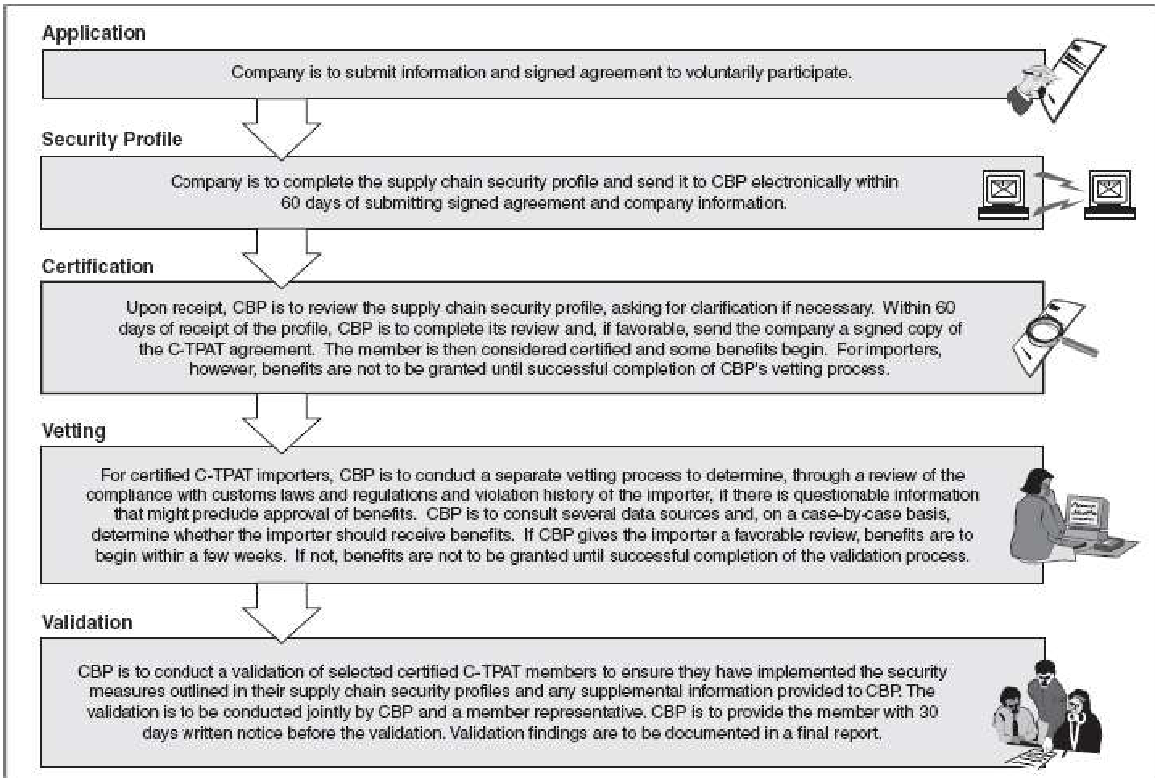
Companies that are interested in becoming a C-TPAT member need to prepare and submit a supply-chain security profile. The profile should include security assessments of foreign facilities, cargo movement and background checks of people across the supply-chain. Currently, C-TPAT members are granted benefits after CBP reviews the profile information provided by the company and the history of compliance with laws and regulations. For importers, benefits may be granted after this review. If CBP is convinced that the

[50] See Footnote 48.

[51] Joseph Martha and Sunil Subbakrishna, "When Just-in-time Becomes Just-in-case", The Wall Street Journal, 22 October 2001.

information provided is reliable and the company has a clean historical record, then the company will start enjoying benefits. Otherwise, CBP performs an additional examination that includes on-site visits and meetings with the company representatives. A final decision is made after this review. The complete review process is illustrated in Figure 5.

Figure 5 CBP's Review Process for C-TPAT Membership[52]



Application

Company is to submit information and signed agreement to voluntarily participate.

Security Profile

Company is to complete the supply chain security profile and send it to CBP electronically within 60 days of submitting signed agreement and company information.

Certification

Upon receipt, CBP is to review the supply chain security profile, asking for clarification if necessary. Within 60 days of receipt of the profile, CBP is to complete its review and, if favorable, send the company a signed copy of the C-TPAT agreement. The member is then considered certified and some benefits begin. For importers, however, benefits are not to be granted until successful completion of CBP's vetting process.

Vetting

For certified C-TPAT importers, CBP is to conduct a separate vetting process to determine, through a review of the compliance with customs laws and regulations and violation history of the importer, if there is questionable information that might preclude approval of benefits. CBP is to consult several data sources and, on a case-by-case basis, determine whether the importer should receive benefits. If CBP gives the importer a favorable review, benefits are to begin withir a few weeks. If not, benefits are not to be granted until successful completion of the validation process.

Validation

CBP is to conduct a validation of selected certified C-TPAT members to ensure they have implemented the security measures outlined in their supply chain security profiles and any supplemental information provided to CBP. The validation is to be conducted jointly by CBP and a member representative. CBP is to provide the member with 30 days written notice before the validation. Validation findings are to be documented in a final report.

iii. Operation Safe Commerce (OSC)

Operation Safe Commerce is currently administered by the Office of Domestic Preparedness. OSC is designed to promote development of technology to improve container security. The goals are to increase the transparency of cargo, employ state of the art technology for inspection, prevent cargo tampering and reduce theft. While CSI and C-TPAT seek to reach out foreign ports and loading facilities to standardize the guidelines for securing container shipments, OSC sets the standards that should be followed during transportation and when the cargo reaches US ports. In short, OSC addresses the question of “What’s in the container?” after it leaves the port of origin. Thus, use of sensors, seals and other cargo tracking and security technology are encouraged under this program. This program also seeks to identify the best technology and practices that prevents cargo tampering.

This program initially began as a partnership between government bodies and private sector to address vulnerabilities in cargo security. OSC consists of three phases. The first two phases were completed by the end of 2004, and involved security assessment of the entire supply-chain. In particular, security assessments at Los Angeles/Long Beach, Seattle/Tacoma and New York/New Jersey ports were

[52] Source: GAO Report, GAO-05-404, “Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security”, March 2005.

completed along with a detailed analysis of the vulnerabilities of 19 separate supply-chains. The best technology and best practices identified in the first two phases are currently subject to further evaluation in the third phase.

Figure 6 Container Loading Operation at the Port of Halifax, Canada[53]

iv. Megaports Initiative

Megaports Initiative is a program to improve radiological material and nuclear weapon detection capabilities at foreign ports. It complements CSI in that cargo is inspected for nuclear and radiological content at the port of origin. The program was initiated with the recognition that it may be too late to respond to a nuclear threat at a domestic port. The ultimate goal is to deter illicit nuclear and radiological material trafficking. The program was initiated in 2003 by the Department of Energy (DOE).

This program consists of six phases:[54] (1) port prioritization; (2) government-to-government negotiations and port familiarization; (3) technical site surveys, site design and training; (4) final design, construction, and equipment installation; (5) equipment calibration and testing; (6) maintenance and sustainability. In order to maximize deterrence of the program, the goal is to inspect all cargo leaving the port regardless of destination. Sandia National Labs use the Maritime Prioritization Model to rank 120 seaports[55] worldwide based on the attractiveness of the port for nuclear smuggling. An interesting characteristic of the model is that ranking is performed based on unclassified information. DOE officials should negotiate with the host governments and port officials and finalize an agreement. The agreement addresses critical issues like equipment needs of the port, placement of equipment, and optimal calibration to detect nuclear and radiological content. Another challenge that DOE faces is training of the personnel. At the end of the fifth

[53] Source: US Bureau of Customs and Border Protection website: www.cbp.gov.

[54] GAO Report, GAO-05-375, “Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports”, 31 March 2005.

[55] This number is expected to increase by 80 during fiscal year 2005.

phase, the host government takes control of all the equipment, but receives support from DOE for maintenance.

As of April 2005, DOE has completed work at 2 foreign seaports: Rotherdam and Piraeus. Although Piraeous was not ranked on the top of the list, it received quick treatment because of security alert during Olympic Games. Agreements are finalized with 5 other seaports and negotiations are still in progress with 18 additional countries.

v. Federal Budget Appropriations for Cargo Security Initiatives

CSI and C-TPAT funds have been continuously increasing over the years. In 2003 CSI budget was $28 million, whereas C-TPAT received $9 million. In 2004, there was a significant increase in appropriations for CSI and C-TPAT programs. Federal government allocated $108.4 million in 2004 and $133.4 million in 2005 on CSI as well as $26.9 million in 2004 and $42.1 million in 2005 on C-TPAT operations.[56] President Bush has further proposed an increase of $5.4 million for CSI and $8.2 million for C-TPAT in 2006 fiscal year budget.

Federal appropriations under OSC support testing and improvement of container security technology. So far, a total of $75 million was allocated to improve port security as a part of the pilot program at ports of Seattle/Tacoma, Los Angeles/Long Beach and New York/New Jersey. $28 million was allocated for the first phase and $30 million was allocated for the second phase. In April 2005, DHS announced the last portion of this $75 million grant, which is $17.1 million.[57] $6.7 million was awarded to Los Angeles/Long Beach, $5.2 million to Seattle/Tacoma and $5.2 million to New York/New Jersey.

Megaports Initiative has received $43 million through the end of fiscal year 2004. It is expected that the program needs $337 million for installation of equipment at 20 additional ports by 2010.[58]

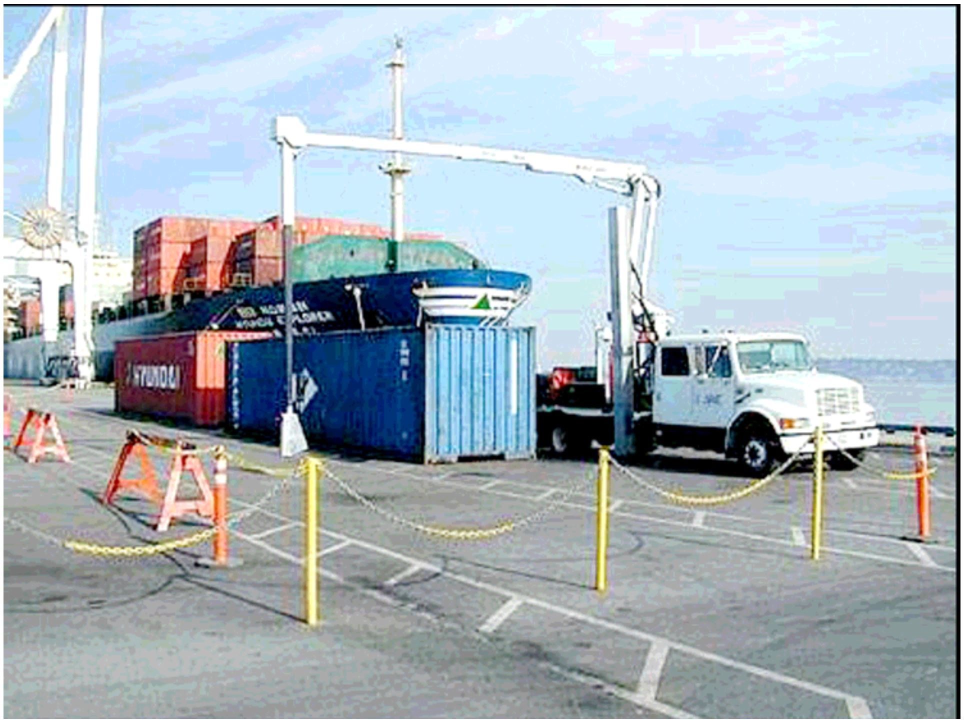
vi. Technology

Huge volume of cargo arriving at US each day makes 100% physical inspection impossible. Thus, the capability to detect illegal contraband in a cargo largely depends on the effectiveness of non-intrusive inspection (NII) technologies. Devices with NII technology encompass X-ray and gamma imaging systems, portable and hand-held radiation detectors, remote monitoring equipment and portal sensors. Likewise, radio-frequency identification (RFID) tags, anti-tamper seals and smart boxes entail better transparency of the entire supply-chain, hence serving for better security.

In a recent Science and Transportation Committee Hearing[59], Executive Vice President of American Association of Port Authorities, Jean Goodwin, provided information about the current status of NII technology deployment to seaports. 59 large-scale NII systems have been deployed to US and Caribbean seaports. The Vehicle and Cargo Inspection System (VACIS), mobile VACIS, truck X-ray, mobile truck X-ray, rail VACIS, mobile sea container examination systems and the pallet gamma-ray system are included in each package. CBP has deployed nuclear and radiological equipment as well. Among these devices are Personal Radiation Detectors (PRDs), Radiation Isotope Identifier Devices (RIIDs) and Radiation Portal Monitors (RPMs). So far, CBP has deployed over 400 RIIDs, nearly 500 RPMs and over 10,000 PRDs. These figures may include those that are shipped to foreign ports.

[56] Congressional Quarterly, http://homeland.cq.com.
[57] Jim Morris, "DHS Announces $17.1 Million in Port Security Grants.", Congressional Quarterly, 14 April 2005.
[58] See Footnote 54.
[59] 17 May 2005, complete testimony can be found at http://homeland.cq.com.

Figure 7 Mobile VACIS[60]



Mobile VACIS devices include truck-mounted, gamma-ray imaging system that takes radiographic snapshots of the containers, highway trailers and passenger vehicles. Scanning of a typical 40 ft. container takes between 30 seconds and three minutes. Relocatable VACIS scan large vehicles and cargo containers up to 70 ft. long. Pallet gamma-ray systems produce the image of fully loaded pallets or pallet-sized containers. For the railroad cars, VACIS inspection is performed as they pass through an inspection area.

PRD is a handheld device developed for safety of the inspection personnel. It can detect radioactive emissions from nuclear sources. RPM, on the other hand, is used to monitor moving vehicles for the radioactive material. Radioactive material detection technology is deployed both to domestic and foreign ports.

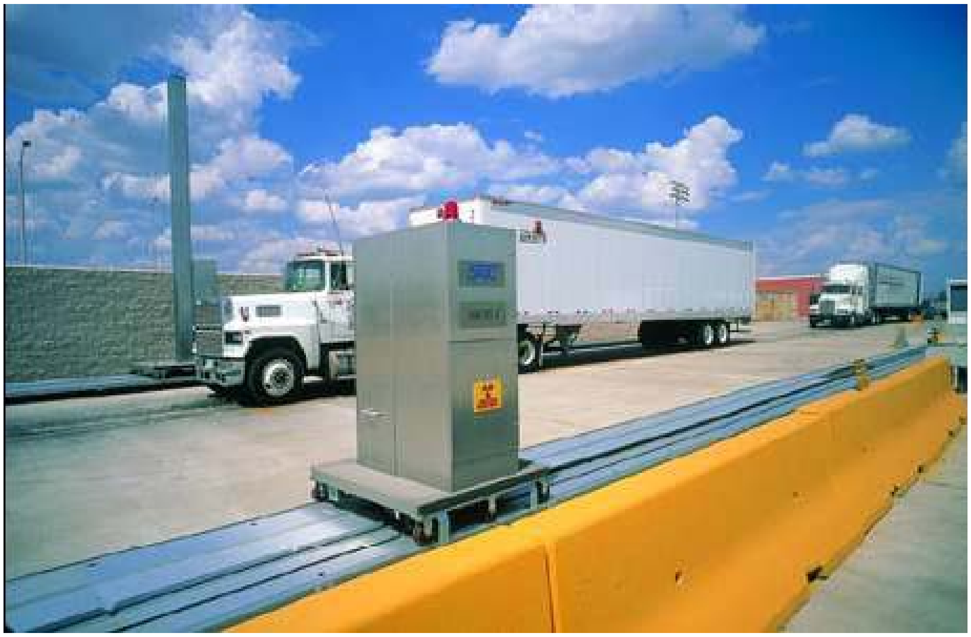
An RFID tag is a microchip with no battery that sends a unique ID code upon receiving a radio query. It is expected to replace UPC bar codes in the near future. RFID tags offer faster scanning of items as multiple items can be scanned at a time. The tracking of inventory is much easier with these smart tags which can receive signals from a long range. These features make RFID technology ideal for checking the contents of the container shipments. The cost per tag varies from 50 cents to $1.[61] Anti-tamper seals, on the other hand, are designed to prevent unauthorized opening of containers. The cost of an anti-tamper seal varies from 10 cents per piece to $25 per piece, depending on the level of security they provide to the container. Both technologies are promoted by CBP to accelerate the development of smart boxes. While there is no standard for what technologies should be available on smart boxes, the intention is to design a container that can signal tampering during shipment. Some experts opt for installation of tracking technology that

[60] Source: www.saic.com.

[61] Manish Bhuptani and Shahram Moradpour, “Time for RFID: Applying RFID in the Supply-Chain”, Supply & Demand Chain Executive, 7 June 2004.

conveys routing information, locating motion detectors inside smart containers or using anti-tamper technology that can transport signals if the container is opened in transit.

Figure 8 Relocatable VACIS[62]



vii. General Discussion on Containerized Cargo Security

While we believe that the efforts by DHS to beef up cargo security after 9/11 should be applauded, as the US Rep. Jane Harman (D-CA) puts it, "our ports remain vulnerable to those who would do us harm or wreck havoc to our economy"[63]. Terrorists seek to develop capabilities to exploit security breach at seaports, and as the Air Force General Ed Eberhart says "…it is just a matter of time until the terrorists try to use a seaborne attack, a maritime attack against us". [64]

Nearly 10 million containers arrive at US ports each year.[65] Only 5% are inspected. CBP is following a layered approach to select and inspect the containers based on the information provided by the shippers, the port of origin and classified targeting rules. Containers from high risk states are subject to inspection.[66] This policy rules out the possibility of shipping lethal contraband from one of these countries to a great extent, as terrorists observe and adapt to new security environment and act accordingly. Terrorists are believed to conduct maritime business and other operations from some of the ports in high risk states, particularly in Indonesia, mainly because of corrupt port authorities.[67] Jemaah Islamiyah, Hezbollah, Al-Qaeda and others have long sought to develop their maritime capabilities across the globe. However, terrorists probably recognize that shipping explosives or weapons from those ports that they are known or

[62] See Footnote 60.
[63] "Harman Applauds $6.7 Million in Port Security Grant Funding", Press Release, www.house.gov/harman , 14 April 2005.
[64] Merrie Schilter-Lowe, "Lack of Maritime Security Leaves US Ports Open to Attack", American Forces Information Service: www.defenselink.mil, 10 September 2004.
[65] Pam Fessler, "Port Security Contingency Plans Scrutinized", NPR Morning Edition, 8 March 2005.
[66] Greg Krikorian, "L.A. Harbor Ports to Get $6.7 Million for Security", Los Angeles Times, 15 April 2005.
[67] Dana Dillon, "Maritime Piracy", SAIS Review, Winter 2005.

believed to be active is not a good strategy for their purposes.

Is it possible to locate explosives or illegal weapons in a container owned by a “trusted” shipper originating from a relatively secure CSI port? Stephen Flynn, a senior fellow in national security studies at the Council of Foreign Relations, describes one such scenario in his book *America the Vulnerable.* In short, terrorists can exploit security gaps during transportation of containers to a CSI port, loading a dirty bomb at a railroad facility. They may target a container from a “well-established manufacturer” which will reduce the probability its selection for inspection. According to the scenario, the shipment originates from Rotterdam. The security breach around this particular port has been confirmed by the recent drug interdiction incident in Australia. Australian customs officials seized 370,000 ecstasy tablets in a Melbourne freight warehouse in a shipment originating from Rotterdam.[68] Likewise, other CSI ports have been vulnerable to drug trafficking in recent years. In June 2002, a shipment of cannabis that originated from Port of Antwerp was interdicted in Ireland.[69] On December 12, 2003, an ecstasy shipment from the port of Tilbury was discovered in Sydney.[70] According to a recent report prepared by the National Criminal Intelligence Service of United Kingdom, “…the use of feeder vessels to transport cocaine from Rotterdam, Antwerp and Hamburg to container ports in southern and eastern England is known to take place.” Furthermore, terrorists have utilized CSI ports for small arms smuggling in the recent past. According to Jane’s Intelligence Review, an arms cache shipped from the port of Hong Kong via Singapore was interdicted in Bangladesh.[71] Terrorists are smugglers still actively operating around CSI ports, and can exploit vulnerabilities on inland or maritime shipping routes to transport weapons and explosives to the United States.

Extending US borders beyond the homeland is a part of layered defensive strategy against terrorism. CSI have partially accomplished this goal by reaching foreign ports. C-TPAT extends the borders further by cooperating with US companies to use their leverage on their global trade partners. While, C-TPAT helped improving security at the loading phase of containers, there is relatively little security improvement in the transportation phase. Supply-chains may not enjoy high level of security during transportation of US-bound containers in foreign countries as the US government cannot reach beyond the ports and foreign private companies may underinvest in transportation security. In particular, those countries with minimal historical exposure to terrorism may overlook some of the key security issues. Cargo theft is a real issue that companies have had to counter for years. The most vulnerable points in the supply-chain to cargo theft are the intermodal transfer locations. Foreign governments have to take the initiative to beef up security at these locations, so that terrorists are deterred from tampering with cargo in transit. Therefore, the US government should pursue a policy that seeks to raise awareness of homeland security issues in foreign countries.

Anti-tamper seals have been developed to ensure integrity of cargo in transit. However, most anti-tamper seals are cheap, and have minimal impact on security. Terrorists can easily break the seal in most cases, and replace it with an identical copy after tampering.[72] Electronic seals can flag an intrusion once they are broken. However, thieves have already developed the expertise to open containers without breaking ordinary anti-tamper seals.[73] Electronic seals are relatively new, but it is still possible to open a container without tampering with these seals. A dirty bomb can be located in a container by removing the doors

[68] 91.7 kg of drugs were hidden in plastic pipes inside eight metal German-made barbecues. Source: “$18 Million Drug Seizure Like a Needle in a Haystack”, AAP General News Wire, 22 April 2005.

[69] “Gardai Question Dutch Man Following Drug Seizure”, www.irishtrucker.com, 22 July 2002.

[70] “Counterdrug Press Summary”, Cubic Analysis Center, 17 November 2004.

[71] BurmaNet News, 3 March 2005.

[72] Stephen Flynn, “America the Vulnerable”, New York: Harper Collins, 2004.

[73] Peter Tirschwell, “No Simple Solutions for Box Security”, Journal of Commerce, 30 October 2003.

completely without breaking the seal.[74] Charles D. Massey, manager of international borders and maritime security at Sandia National Laboratories, claims that a Sandia technician can easily pass electronic seal barrier in a couple of minutes.[75]

Likewise, Global Positioning System (GPS) and RFID technologies do not guarantee the integrity of containers. GPS is a device that electronically reports the position of the container in transit. Both provide good surveillance as to determine where the container is and to improve transparency, however, a terrorist can get away with this problem by placing the bomb by partially removing the contents of the container. Unless both technologies are made smarter, terrorists will be able to tamper with the container unnoticed.

Installation of electronic sensors in containers is another option. However, this technology is still under development phase and the rate of false alarms is high.[76] CBP seeks to reduce the false positive rate to 1% or less. Another drawback is the cost. According to Stephen Flynn, cost of all the equipment that monitors position and integrity of the cargo will be in $100-$200 range.[77] He further estimates that electronic sensors for chemical or radiological materials in a container cost $50. Including the maintenance cost per year, technology will cost $10-$20 per shipment, and Stephen Flynn is optimistic that this will be acceptable range as it will have “no measurable impact” on world trade. However, given that companies today are hesitant to replace bar codes which cost next to nothing with RFID tags that cost less than $1 per tag, regulations may be required to install high-tech sensors.

In a recent article in Journal of Commerce, General Electric is reported to be developing a new technology, Container Security Device (CSD), to detect intrusion. CSD sends alert signals whenever a box is entered. This technology will monitor all six sides of the container. The device will be sold for $50 and will be good for at least 10 years. If this technology works as intended, it may be a good security solution for the cargo in transit.

A recent GAO testimony[78] highlights some of the weaknesses in the implementation of the C-TPAT program. GAO review of the program shows that the validation phase is not based on an independent audit. GAO believes that guidelines are insufficient, and in most cases the performance criteria that should be met to receive C-TPAT benefits are jointly agreed upon with the member company. Another significant weakness highlighted in the testimony is staff shortages to perform validations. Only 11% of the certified members are validated. Furthermore, GAO criticizes the lack of performance measures and an effective records management system.

Oakland has recently become the first port with %100 radiation inspection capability in the nation.[79] The ultimate goal is to install radiation portal monitors at every port in the United States to ensure that %100 of cargo containers are inspected for radiation. As intermodal transportation becomes the regular means to ship goods across the globe, threat posed by radiological bombs extends from shores to central homeland. Most containers are destined to inland ports either on trucks or on rail. Thus, it is possible to ship dirty bombs to inland targets if seaports are not armed with %100 radiation inspection capability. The federal government is aware of this issue and deploys more resources for radiation detection technology.

[74] Bob Durstenfeld et al., “Cargo Container Security”, Occupational Health & Safety, August 2003.
[75] R.G. Edmonson, “Still Trying on E-seals”, Journal of Commerce, 16 May 2005.
[76] Peter Tirschwell, “Progress on Container Security”, Journal of Commerce, 20 September 2004.
[77] Corie Lok, “Cargo Security”, Technology Review, June 2004.
[78] GAO Testimony, GAO-05-466T, “Homeland Security: Key Cargo Security Programs Can Be Improved”, 26 May 2005.
[79] Paul Rosynsky, “Oakland Port Gets Radiation Detectors”, Paul T. Rosysnky, 27 April 2005.

However, current radiation portal monitor technology does not guarantee an acceptable detection rate even when all the maritime ports are completely covered. Highly enriched uranium is not necessarily detected by the current technology. In this sense, "radiation portals have limited utility."[80] Another concern about the technology is high rate of false positives. Customs officials in Newark have reportedly nicknamed these devices as "dumb sensors" because they cannot identify the source of radiation correctly.[81] Items such as granite, porcelain toilets and bananas can set off a radiation alert. Too many false positives hamper smooth flow of trade at seaports. A %100 inspection policy has the same drawback. However, customs officials believe that the current state of disruption is not likely to make a big impact on trade.[82]

There is no effective detection equipment for biological and chemical weapons. Since chemical sensors are not regularly installed in the containers, the only way to interdict shipment of a chemical weapon is to catch anomalies in gamma-ray images of the container. Inspectors may fail to spot anomalies in gamma-ray images.[83] As far as biological weapons, the level of vulnerability is higher as there is no effective sensor in the market for biological contaminants.

There are some other challenges related with the CSI program. The success of this initiative relies on the level of cooperation provided by the foreign port officials. According to the current procedure, when a high risk cargo is identified, the foreign customs' officials are responsible for inspection and US officials are entitled to observe the inspection process. However, according to recent reports, US officials' role in this inspection process has been relegated to the review of cargo manifests.[84] Some foreign ports, such as Le Havre in France, perceive monitoring by US officials as violation of sovereignty. Since the US government is unable to perform background checks for foreign port workers, observing the inspection process is an important element of CSI.

As of September 2004, 65%[85] of the containers originated from CSI ports (which constitute 43% of all shipments to the United States) have been subject to targeting using the ATS system, which implies that the remaining 35% were not subject to any risk assessment and inspections overseas. GAO attributes this to staffing imbalances at the CSI ports. 72% of the high risk containers were inspected overseas, and the rest were denied inspection based on a variety of reasons. Of the remaining 28%, %93 was inspected upon arrival at a US port. The remaining 7% were not subject to any inspection for either due to lowered risk score based on further incoming intelligence, or because the port of destination was other than a US port. It should be noted that, further cooperation from foreign port officials is required as it may be too late to respond to the terrorism threat.

Currently, ATS and intelligence reports are used to assign a risk score to incoming cargo. According to GAO, there are implementation problems in ATS, as CBP has not conducted a risk characterization of different forms of cargo and different transportation modes.[86] This requires expertise in commercial shipping and supply-chain operations. The development of this expertise has been rather slow.[87] The CBP officials

[80] Stephen Flynn has made that comment. Peter Tirschwell, "Nukes and Container Security", Journal of Commerce, 28 March 2005.

[81] Eric Lipton, Matthew L. Wald, "US to Spend Billions More to Alter Security Systems", New York Times, 8 May 2005.

[82] Ronald D. White, "Detectors May Cause Port Delays", Los Angeles Times, 7 May 2005.

[83] Fen Montaigne, "Policing America's Ports", Smithsonian, January 2004.

[84] Caitlin Harrington, "Concern Grows Over Gaps in Foreign Port Screening", Congressional Quarterly, 17 May 2005.

[85] GAO Report, GAO-05-557, "Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts", April 2005.

[86] GAO Testimony GAO-04-325T, "Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers", 16 December 2003.

[87] Carl Bentzel, a senior advisor at Transportation, Infrastructure & Homeland Security Group, has noted that the

should point to anomalies in shipment routes to detect possible intrusion into containers or loading of illegal contraband during visits to ports en route. Without providing such training to customs personnel and understating the human element in successfully targeting containers, risk scores will have deficiencies. Another implementation problem for ATS is its reliance on the information provided by the shippers. Without installing GPS to improve transparency, there is no way to verify the accuracy of the route information.

Use of technology for cargo inspections overseas is not problem free either. Apart from the limitations of device used for inspections to detect illegal weapons or explosives, the sensitivity of the equipment to detect anomalies is under the control of foreign port officials. For instance, foreign port officials may choose to reduce the sensitivity of RPM equipment if the number of false alarms hampers the flow of trade. US officials have no control over the equipment after their calibration and testing is completed. Another factor that could limit the effectiveness of the equipment is the environmental conditions. RPMs tend to be less effective in cold and windy climates. In general, it is difficult to measure the effectiveness of radiological and nuclear content detection equipment installed at foreign imports under Megaports Initiative. Other factors that limit the effectiveness of this initiative are its very limited coverage and slow progress in installations due to operational difficulties.[88]

At the opposite end of the spectrum are the empty containers. Currently, empty containers are not checked at all.[89] A popular metaphor, Trojan Horse, which is used for containers in the context of port security, should in reality be used for empty containers as the original Trojan Horse was thought to be empty. One port worker says: “Prior to September 11, part of our function in the harbor was to open these containers and look inside to make sure that they were clean.” A particular vulnerability with respect to empty containers is the lack of any protocol or a requirement to lock them in transit. Thus, it is relatively easy to place a bomb into these containers. We can easily recognize the urgency to address this issue as the 40% of the containers present at a West Coast port on a given day is empty.[90] Empty containers may lie unattended at the port facility for days. One reason for ignorance on the issue is that most empty containers are outbound. However, ports may be targets themselves of a terrorist attack. In that regard, this vulnerability can easily be exploited by a terrorist to detonate explosives and disrupt port operations for a period of time. According to Michael Mitre of ILWU, checking empty containers is much easier than checking a loaded container. We should quickly adress this issue by standardizing treatment of empty containers at the port facilities. It seems that after 9/11, ports have become more secure at some of the vulnerable points at the expense of leaving no defense system at some others, possibly because of limited resources.

Another piece of container security paradigm that has been largely overlooked in the past is the export cargo. With the implementation of CSI and 24-hour rule, inbound containers with manifest such as “freight of all kind” were no longer allowed in US ports. This kind of description does not provide any information on the actual contents of the container. However, containers with such descriptions are still allowed for export cargo. This is a perfect opportunity for a potential terrorist attack. A container explosion incident at the Port of Los Angeles in 2004 was a warning sign.[91] An outbound container which carried hazardous material

government does not understand the maritime environment well. He made these comments at the Maritime Security Conference on May 2, 2005 in Arlington, Virginia.

[88] GAO Report, GAO-05-375, “Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports”, 31 March 2005.

[89]Alex Chadwick and Noah Adams, “Megaships: Tying Asia to Southern California”, NPR Day to Day, 26 November 2004.

[90] Congressional testimony on maritime security to Committee on House Transportation and Infrastructure by Michael Mitre. Michael Mitre is the port security director of International Longshore and Warehouse Union (ILWU).

[91] Ibid.

exploded when it was laid unattended for three days at the port without any special precautions taken because the cargo was supposedly "freight of all kind". Michael Mitre of ILWU proposes banning practice of vague descriptions for export cargo and extending the 24-hour cargo manifestation rule to cover all containerized cargo moving through ports. In other words, his proposal is to make sure cargo manifest information arrives 24 hours before the cargo is delivered to the port by either truck or rail. We believe this policy could reduce the terrorism threat from an export cargo.

III. Vulnerabilities and Policies in General Cargo Security

General cargo category encompasses liquid bulk (such as petroleum), dry bulk (such as grain, paper), and iron ore or steel loads which are generally not shipped in containers. General cargo ships were used historically to smuggle drugs and other contraband.[92] Cocaine smugglers are known to prefer shipping their cargo disguised in iron ore or charcoal shipments because of relatively low probability of detection.[93] However, general cargo shipments may not provide the same level of convenience in weapons smuggling as containerized shipments. The only incentive for weapons smuggling in a general cargo ship would be relatively high detection rate for weapons smuggling in containers.

General cargo ships have been used for terrorism purposes, too. In 2002, Italian officials arrested 15 Pakistani men with false passports and suspicious documents on a Tonga-registered vessel carrying a cargo of lead.[94] They were suspected to have links with Al-Qaeda. In November 2001 a Cambodia-registered vessel, supposedly carrying a cargo of timber, was found to smuggle cigarettes in Ireland to finance Real IRA operations.[95] In 2002, a general cargo vessel (named Karine A) loaded with 50 tons of weapons was captured by Israeli officials.[96] Among the weapons were 122mm Katyusha rockets, 107mm rockets, 120mm mortars, Sager and LAW anti-tank rockets, mines, sniper rifles, Kalashnikov assault rifles, bullets and explosives.

While considerable attention has been warranted on container security, general cargo has received little interest, at least in the media. All vessels that transport goods to the United States have to report their cargo information 24 hours before they leave the port of origin and the arrival schedule 96 hours before they arrive at a US port. Those vessels whose schedule of arrival has not changed more than 6 hours are not required to submit an update. The arrival schedule is reported filling ANOA document, which requires information about the last 5 ports of entry. If a ship is bound to visit multiple ports in US, it has to file a new ANOA for every single port. The goal is to determine the route of the vessel in order to assign a risk score. Vessels larger than 300 gross tons file this document with National Vessel Movement Center (NVMC).

For vessels that are less than 300 gross tons, an ANOA is not required. However, some ports may choose to ask for ANOA information.[97] However, US-flag recreational vessels are exempt from this requirement. Most commercial vessels that are less than 300 gross tons are fishing boats. Inspection will be triggered if

[92] For instance, Coast Guard found 10,000 pounds of cocaine hidden below iron ore pellets in 1999. For more info, please see: "Drug Ship Auction in Texas Draws Bidders Worldwide", Knight Ridder Tribune, 26 May 1999.

[93] "Agents Adapt to Changing Tactics in Drug Smuggling", States News Service, 4 May 1999.

[94] "Italy arrests 15 Pakistanis suspected of Al-Qaeda links, terror plans", Agence France Presse English, 12 September 2002.

[95] "Raid at Sea Highlights Flag Abuses: Cambodia-listed Ship was Carrying Cocaine", International Herald Tribune, 24 June 2002.

[96] "Israel Seizes Palestinian Gun-Running Ship", United Press International, 4 January 2002.

[97] For instance, Port of Los Angeles does not require this information, whereas US Coast Guard in South Florida began to enforce the rule on May 21, 2004. The vessels have to file ANOA with the captain of the port. For details, please see Lucy Chabot Reed, "No ANOA Needed for Pleasure Vessels Coming to South Florida.", www.the-triton.com.

given the information from ANOA or other intelligence information, a vessel is believed to engage in an illegal activity. Without ANOA, the route information for general cargo ships won't be known. This creates another pathway to introduce a dirty bomb or an illegal contraband into the United States. The risk is particularly high for ships carrying hazardous cargo. Terrorists may have interest to explode ships carrying hazardous cargo for inflict more damage. Since most of the attention is warranted on container security, a bulk cargo vessel with illegal contraband may be unnoticed. Therefore, ANOA requirement should be extended to all vessels that enter seaports.

General cargo ships may themselves be used as weapons to attack coastal targets, or as indicated above to explode a bomb. These scenarios are discussed in later sections as targets of such attacks may be coastal facilities other than ports.

b. Security of Port Area and Perimeters

Historically, illegal drugs and other contraband have been frequently shipped disguised among legitimate cargo. On the other hand, maritime terrorists have so far not attacked maritime ports. However, Americans have every reason to fear that an attack on the United States may be launched from port perimeters or inside a port area, possibly delivering a more devastating blow than a cargo attack. Huge number of critical infrastructure around maritime ports and vast size of the perimeter area that needs protection augment this fear. Realizing that port facility is only as secure as its perimeter, we need to develop systems that would deter, detect, document and deny any unauthorized entry to port area and its perimeters. In this section, current status of security measures to address terrorism threat is discussed.

I. Access to Secure Areas

Human element is critical ensure security at a port area. The goal is to deny access to those who are not authorized and have criminal background to secure areas around maritime ports. USA Patriot Act of 2001 requires background checks for all those individuals involved in transportation of hazardous materials in commerce. Ports are among the intermodal sites where tons of hazardous materials cross. This legislation was customized to the maritime environment by the Maritime Transportation Security Act of 2002. The act requires issuance of transportation security cards with biometric information and an overall background check for all workers employed at maritime ports. Otherwise, those with criminal records or those who have stolen identity can get an access to secure areas in maritime ports.

In the current system, verification of identity is achieved by checking photo ID, which does not require any background check or check against national security databases. Obtaining a driver's license did not even require a legal status in the United States until recently.[98] In the old system, consular cards issued by other countries such as Mexico would be sufficient to issue a driver's license. This opened the door to illegal aliens to get jobs in port areas. TSA is planning to overcome this identity problem by designing Transportation Workers Identification Card (TWIC) that will be issued to all the 12 million transportation workers who needs an unescorted access to secure areas. These cards will have fingerprint information embedded and be tamper resistant. DHS's fiscal year 2006 budget request includes around $245 million for TWIC.

Progress towards use of TWIC has been rather slow. TSA awarded $12 million contract to Bearing Point in

[98] President George Bush signed a legislation that standardizes the procedures across all the states. The legislation became effective on May 11, 2005. Under the current legislation, the driver has to provide a birth certificate, proof of SSN, a photo ID and a document with their name and principal address. Kevin Murphy, "New Rules Will Make Your Driver's License Harder to Get", The Kansas City Star, 20 May 2005.

August 2004, and launched a prototype TWIC program at four sites in November 2004.[99] When TSA initiated TWIC program in 2002, the plan was to issue first cards in August 2004.[100] However, as Margaret Wrightson, director of homeland security and justice issues at Government Accountability Office said "We are now nearly halfway through 2005 and TWIC is still in the prototype phase, with critical policy decisions still to be made."[101] Delay was partly attributed to the late decision on the type of technology to use, late approval by DHS to conduct prototype test and data challenges.[102] In order to mitigate risks due to delays, TSA is currently requiring the transportation workers to carry different identification cards for each facility they access.[103] However, without full implementation of TWIC program, access to secure areas at maritime ports will remain to be a vulnerable point of the system.

Figure 9 Aerial View of the Port of Long Beach[104]

Every year, approximately 7,500 foreign flagged ships visit US ports, carrying the bulk of shipment to the United States including 175 billions gallons of oil and other fuels.[105] 93% of US the trade sails over non US-owned or non US-flag ships with foreign crew. Before 9/11, foreign crew could get a visa without visiting the embassy or consular office in person as the shipment companies could obtain visas for all crew members by submitting list of the crew to a US embassy. This vulnerability was addressed by requiring all foreign members acquire their own visas. However, threat posed by stowaways remains unless port surveillance

[99] www.bearingpoint.com.

[100] GAO Report GAO-05-106, "Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program", 10 December 2004.

[101] Congressional Hearings on port security issues, 17 May 2005.

[102] GAO Testimony GAO-05-357T, "Transportation Security: Systematic Planning Needed to Optimize Resources", 15 February 2005.

[103] www.globalsecurity.org.

[104] Port of Long Beach website, www.polb.com.

[105] Council of Foreign Relations Terrorism Website, www.cfrterrorism.org.

capabilities are improved and access to secure areas is granted with state of the art identification cards. Terrorists may use this route that has been historically utilized by human smugglers to either sneak through the border, or launch an attack in the port area. They may seek cooperation with the foreign crew with sympathy towards their agenda to board the ship and penetrate through the port facility when the ship arrives at a port. Furthermore, at the federal level, there does not seem to be any effort to incentivize US shippers to enlarge their commercial fleet or to encourage US vessel owners who operate their ships under foreign flags to switch to American flag.

Port officials have taken steps to install new technology to improve surveillance capabilities in the port area. So far, some ports have installed integrated security management systems that have video surveillance, automated access control and perimeter intrusion detection capabilities.[106] These are positive steps to minimize the risk of authorized access to secure areas in a port. However, these technologies also have limitations. As in the case of RPM, most sensor technology comes with the dilemma of sensitivity adjustment vs false alarm rate. For example, motion sensors can be adjusted to track a flying bird, wall vibration sensors may react to any vibrating object or machinery and ultrasonic sensors may detect any noise in the ultrasonic range. In order to reduce the time to identify false alarms, cameras may be installed around sensors. However, lights may change the thermal environment and affect the operation of sensors. It is beyond the scope of this report to evaluate alternative technologies or to provide an expert criticism on their defects.[107] A comprehensive terrorism risk assessment of each port area should be done after security improvements are in place to further seal vulnerable points of the whole system. A layered monitoring approach will reduce the likelihood of success for an intrusion attempt.

II. Port Perimeter

Port police and the Coast Guard are responsible for policing waterways inside and around every port. Many naval vessels, commercial vessels with hazardous material, nuclear power plants, densely populated areas and critical infrastructure such as bridges are located on or near the open water ways. A discussion on vulnerabilities at coastal targets is provided later in this report. Since there is a good amount of overlap between two issues, the discussion on port perimeter security is postponed to a later section where risks to all coastal targets are evaluated.

c. Cruise Lines

Hijacking of passenger vessels has been recorded in the past to accomplish political goals. Like airplane hijacking incidents, they attracted a lot of attention, which helped spread the political message of terrorist groups. Cruise ships are enticing targets for terrorists for multiple reasons. First, terrorists can hijack cruise liners for simply piracy and looting purposes because there is a wide belief that cruise ship passengers are rich. Second, some cruise ships have around 5000 passenger capacity. Hence, a single terrorist attack on a cruise ship has the potential to claim thousands of American lives. Such an attack would have ripple effects at least on tourism, aviation and entertainment industry. In this regard, a well organized attack on a cruise liner will fulfill both objectives of terrorists: economic damage and high number of casualties. If terrorists aim at killing the maximum number of people, cruise ships may suffer either seaborne or aerial attacks. It is less likely that cruise ships will be used as weapons themselves. A hijacking incident won't remain as a secret for long, and port officials will have enough time to secure the critical targets on the coast.

[106] An example to that is Port of Oakland. “Port of Oakland Selects ADT to Design and Install a $4.75 Million Maritime Security System”, PR Newswire, 07 May 2003. Port of Galveston, Toledo, and Los Angeles/Long Beach are also among those that installed similar systems.

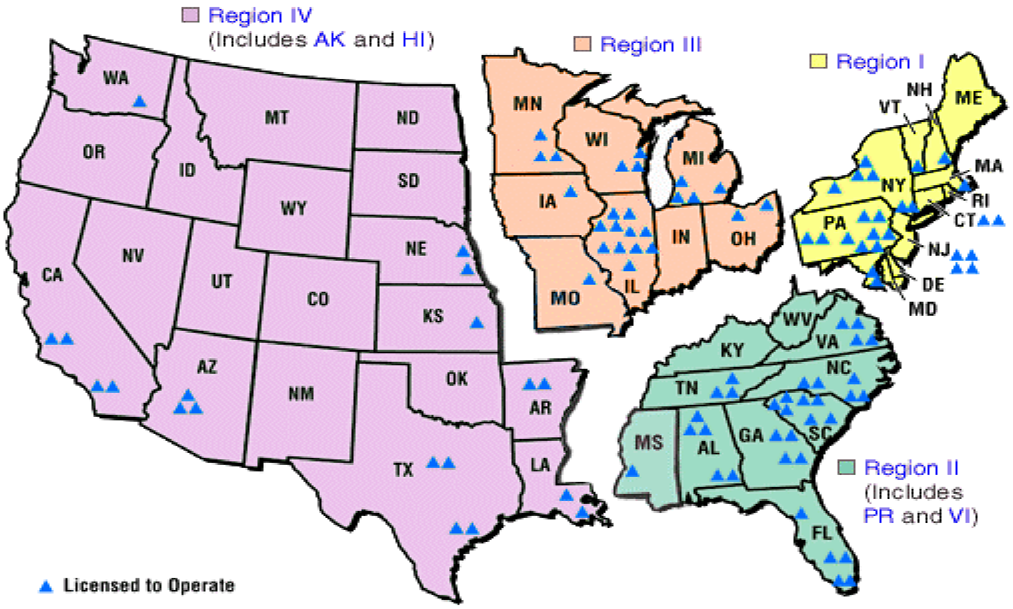
[107] A brief overview of some perimeter security technologies can be found at www.justnet.org/perimetr/full2.htm#tr_9

After the 1985 hijacking of Italian cruise liner Achille Lauro, the cruise industry has implemented a wide array of new anti-terrorism measures. Since 1985, there has been only one cruise ship hijacking incident.[108] In the current era, hijacking of cruise ships in the United States seems less likely, as the cruise liners have adhered to even more strict security measures after 9/11. Specific measures that are enforced by the US Coast Guard include:[109]

- Screening of all the passenger baggage, carry-on luggage and ship cargo. Metal detectors, X-ray machines, human searches and canine teams are used to do screening.
- Screening of passenger lists against criminal and terrorist watch lists.
- Restricting access to secure areas in the port and on the vessel.
- Maintaining a 100-yard security zone around cruise ships.
- Underwater surveillance at high risk ports.

There is no doubt that these security measures have been effective in reducing terrorism risk on cruise liners. The degree of vulnerability to a terrorist attack is more a function of technology failure risk which is and will be present in most security systems. Cruise lines are relatively more secure component of the entire border security system.

Figure 10 Locations of Nuclear Power Plants in the United States[110]



Note: There are no commercial reactors in Alaska or Hawaii.

2. Security of US Waters and Coast

Most US energy power plants, critical bridges and densely populated urban areas lay close to waterways. For instance, 75% of oil refineries and a great majority of 103 nuclear reactors and all LNG terminals in the

[108] "Security Experts Says Cruise Ships a Soft Target for Terrorist Attacks; Industry Says Ships Have Never Been Safer", AP Worldstream, 20 November 2001.
[109] Tim Rubacky, "How Safe are we at Sea?", www.cruisemates.com.
[110] Source: US Nuclear Regulatory Commission website: www.nrc.gov.

United States are located onshore. Nearly all major cities are accessible by waterways. Operation of the infrastructure onshore is crucial for the US economy. A single attack on any of this infrastructure is likely to render a significant number of direct and indirect casualties. Furthermore, they are easier to penetrate from the shore. Thus, they may be attractive targets for terrorists.

a. Discussion of the Coast Guard Capabilities

The Coast Guard currently assumes homeland and non-homeland security responsibilities such as enforcing security laws around ports, waterways and coastlines, interdicting drug and human smugglers, monitoring fishing areas, responding to pollution and conducting search and rescue operations. All these missions are accomplished with a fleet of 186 aircraft, 88 cutters, over 300 patrol boats and 90 special purpose vessels such as icebreakers. A description of the Coast Guard operations is provided in Table 8. Before 9/11, most Coast Guard operational hours were dedicated to search and rescue missions along with three categories of law enforcement: protecting fisheries, interdicting illegal migrants at sea and controlling the flow of drugs. As 9/11 shifted focus on preventing terrorism, Coast Guard resources were largely allocated on homeland security related activities while some of the traditional missions such as search and rescue underwent a significant reduction in operational hours.[111]

The Coast Guard was appropriated $1.5 billion between 2002 and 2004 for equipment replacement and modernization under Deepwater Acquisition Program (DAP) which was initiated in 1996. The program seeks to modernize ships and aircraft used in missions that cannot be carried out by shore-based small boats. The equipment replacement and modernization phase under DAP began in 2002 as the contract for acquisition and integration of necessary equipment was awarded to Integrated Coast Guard Systems. In 2005, DAP was awarded $700 million, making the total funding figure $2.2 billion since the beginning of replacement and modernization phase. $1.3 billion was allocated for new acquisitions and $460.5 million was spent for upgrades on legacy assets. The rest of the funds were used on maintenance operations. A total of $966 million is requested in 2006 as there is an ongoing need to increase the size of the fleet.[112] Another modernization program in progress is Rescue 21, which will replace the equipment used for coastal communication needed for search and rescue operations. $101 million of the budget requested for 2006 will be dedicated to acquisitions under Rescue 21. Total funds requested for fiscal year 2006 amount to $8.1 billion, which constitute 20% of the DHS budget.[113]

According to GAO, the Coast Guard faces challenges in implementing both DAP and Rescue 21. GAO believes that DAP has not enjoyed a predictable and steady funding stream which is key to acquisition and integration of the new equipment to the system. Furthermore, they say that the acquisition program is behind the schedule and pouring more money into the program will not help get inline with the original schedule.[114] Due to these delays, GAO estimates that the cost projection of the program that was originally expected to be $15 billion at the end of 20 years has first risen to $17.2 billion and then recently up to $24 billion. The approach adopted by the Coast Guard in managing this huge acquisition project to hire a single systems integrator led to concerns about potential lack of competition in later phases of asset procurement

[111] According to a GAO report in 2004, this reduction amounted to 22%. Other non-homeland security missions with similar reduction in operational hours are law enforcement activities protecting living marine resources and foreign fish enforcement.

[112] GAO Testimony, GAO-05-307T, “Coast Guard: Preliminary Observations On the Condition of Deepwater Legacy Assets and Acquisition Management Challenges”, 20 April 2005.

[113] GAO Testimony, GAO-05-364T, “Coast Guard: Observations On Agency Priorities in Fiscal Year 2006 Budget Request”, 17 March 2005.

[114] GAO Report, GAO-04-695, “Coast Guard: Deepwater Program Acquisition Schedule Update Needed”, 14 June 2004.

which may eventually lead uncontrolled stream of acquisition costs. This prediction is realized in the earlier years of the project as the estimated cost of the project increased up to 60%. Another reason behind these escalating costs lies in deepwater aircraft and cutters “failing at an unsustainable rate,”[115] which compelled the Coast Guard to revise its implementation plan for this acquisition project. However, the House Appropriations Committee was not satisfied with the plan and recommended that the Coast Guard’s DAP budget request of $966 Million for 2006 be turned down. They proposed a budget of $500 Million which was well below the Coast Guard’s request and the minimum amount required to finish the project within the original 20 year span. Senate Appropriations Committee shared similar concerns, but did not recommend an extensive cut in the budget.

Similar problems have aroused in Rescue 21 program which hampered search and rescue operations across US waters. These problems raise concerns about the capability of the Coast Guard to achieve some of its missions. GAO has also reported that most missions may also suffer from lack of station readiness due to staffing and training problems which lead to prolonged periods of work and shortage of experienced personnel.[116] While the Coast Guard responded to these problems by increasing its operational efficiency through improved technology, port security assessments, stronger partnerships and better information sharing, most of these improvements have remained rather local and should be spread all over the maritime security spectrum.

The Coast Guard is currently developing the operational requirement for Automatic Identification System (AIS). International Maritime Organization's (IMO) package of security measures which extended Safety of Life at Sea (SOLAS) in 2002 included installation of AIS technology as a ship related provision. These security measures that are known as International Ship and Port Facility Security Code (ISPS) required AIS to improve monitoring of vessel movement. AIS is a technology that enables tracking of vessels by coastal stations and other Coast Guard vessels using a portion of radio frequency spectrum for communication. Information such as size of the ship, its course and speed, registration number and other identifying characteristics of vessel can be transmitted to the central Coast Guard location using AIS. This technology is required on all vessels over 300 gross tons. These larger vessels are currently documented by the Coast Guard. The Coast Guard is still developing operational requirements of AIS technology and evaluating these requirements with all the stakeholders involved. AIS is crucial to identify all high tonnage vessels in US waterways and accordingly will help the Coast Guard extend waterways coverage. According to the Coast Guard, an approved AIS equipment price ranges between $3000 and $9000 excluding the installation cost. These price figures for the equipment makes expansion of AIS requirement to vessels below 300 tons costly prohibitive, as most vessels below 300 tons are not commercial. AIS will be implemented in 10 critical maritime areas, which is only a fraction of over 12,000 miles of coastline and 25,000 miles of river and inland shoreline.[117] These areas are currently monitored by radar based Vehicle Traffic Service (VTS) systems.

Smaller vessels which will not be required to install AIS technology are registered by the individual states. Integration of this data into the Coast Guard’s database of vessel registry is crucial to increase the awareness of all the vessels in the maritime domain. The Coast Guard faced problems in the past to

[115] GAO Report, GAO-05-757,”Coast Guard: Progress Being Made on Addressing Deepwater Legacy Asset Condition Issues and Program Management, but Acquisition Challenges Remain”, 22 July 2005.

[116] GAO Report, GAO-05-161,”Coast Guard: Station Readiness Improving, but Resource Challenges and Management Concerns Remain”, 31 January 2005.

[117] These areas cover 10% of the US ports recognized by the Department of Transportation. Some of the major US ports are not involved in these 10 maritime areas. GAO Report, GAO-04-868, “Maritime Security: Partnering Could Reduce Federal Costs and Facilitate Implementation of Automatic Vessel Identification System”, July 2004.

integrate state vessel registry data.[118] Furthermore, there is no legal requirement for individual states to share their vessel registry data with the Coast Guard. These legal boundaries may reduce the capability of the Coast Guard to monitor small vessels that may be involved in illicit arms and contraband traffic.

Table 8 The Coast Guard Missions[119]

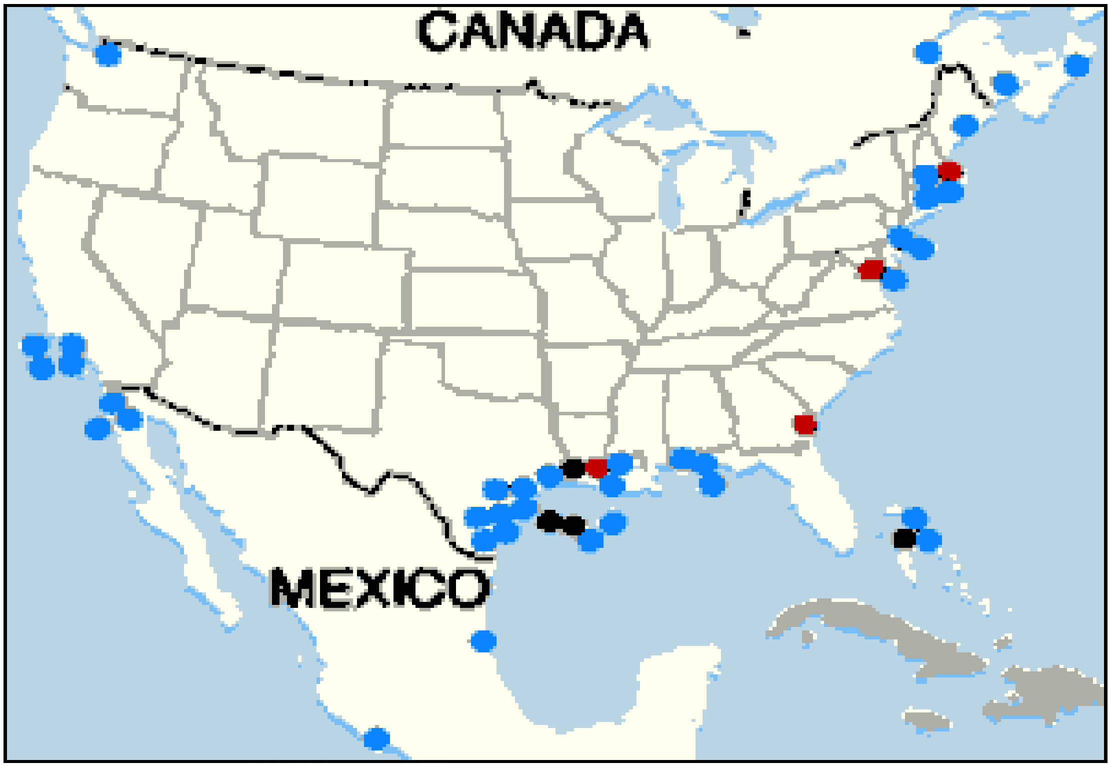
Mission and programs	**Activities and functions of each program**
Homeland security mission	
Port, waterways and coastal security	Conducting harbor patrols, vulnerability assessments, intelligence gathering and analysis, and other activities to prevent terrorist attacks and minimize the damage from attacks that occur.
Illegal drug interdiction	Deploying cutters and aircraft in high drug trafficking areas and gathering intelligence to reduce the flow of illegal drugs through maritime transit routes.
Undocumented migrant interdiction	Deploying cutters and aircraft to reduce the flow of undocumented migrants entering the United States by maritime routes.
Defense readiness	Participating with the Department of Defense (DOD) in global military operations, deploying cutters and other boats in and around harbors to protect DOD force mobilization operations.
Other law enforcement	Protecting US fishing grounds by ensuring that foreign fishermen do not illegally harvest US fish stocks.
Non-homeland security mission	
Search and rescue	Operating multi-mission stations, and a national distress and response communication system, conducting search and rescue operations for mariners in distress.
Living marine resources	Enforcing domestic fishing laws and regulations through inspections and fishery patrols.
Aids to navigation	Managing US waterways and providing a safe, efficient, and navigable marine transportation system; maintaining the extensive system of navigation aids; monitoring marine traffic through vessel traffic service centers
Ice operations	Conducting polar operations to facilitate the movement of critical goods and personnel in support of scientific and national security activity and conducting domestic and international icebreaking operations to facilitate year-round commerce.
Marine environmental protection	Preventing and responding to marine oil and chemical spills; preventing the illegal dumping of plastics and garbage in US waters and preventing biological invasions by aquatic nuisance species.
Marine safety	Setting standards and conducting vessel inspections to better ensure the safety of passengers and crew aboard commercial vessels, cruise ships, ferries, and other passenger vessels and partnering with states and boating safety organizations to reduce recreational boating deaths.

[118] GAO Report, GAO-02-477,"Coast Guard: Vessel Identification System Development Needs to be Assessed..", 24 May 2002.
[119] GAO Report, GAO-04-432,"Coast Guard: Relationship Between Resources Used and Results Achieved Needs to be Clearer.", 22 March 2004.

b. Vulnerabilities along US Waterways and Countermeasures for Risk Mitigation

In this section, we analyze vulnerabilities of three border security sub-components: critical coastal targets, pleasure/fisher boats security and waterways/underwater security.

Figure 11 Approved (black), Proposed (blue) and Existing (red) LNG Terminals in North America[120]



I. Critical Coastal Targets

Maritime terrorism hit US and non US coastal infrastructure in the past. As Figure 10 and Figure 11 illustrate, terrorists have plethora of potential targets for launching deadly attacks on the US coast. The number of potential targets is likely to increase as all new LNG facility locations are proposed to be around the coast. History of maritime terrorism suggests that terrorists have already exercised a variety of options to execute such attacks. In recent years, many terrorist organizations have added various means of suicide attacks in their portfolio of evil deeds. This poses further challenges to those who seek to deter terrorists from attacking one of the most vulnerable points of the nation.

Al Qaeda is believed to control some 15 ships which fly Yemen and Somalia flags.[121] Osama Bin Laden's network can increase the size of this fleet by piracy and further acquisition of new ships. New members of the fleet can be used for an attack before they are identified as a threat. Another option is to smuggle humans on vessels that are destined to sail near the target of interest. Piracy is a rising threat across the globe, and terrorists are already known to use piracy for financing purposes. Likewise, Al Qaeda has already used LNG tankers to smuggle agents to Boston from Algeria.[122] Human smuggling on ships

[120] Source: www.mindfully.org.
[121] Gary Jones, "Osama's Navy", Daily Mirror, 12 February 2004.
[122] Mark Clayton, "LNG: A Prized Energy Source, or Potent Terror Target?", Christian Science Monitor.

carrying hazardous cargo becomes a real issue when we consider the percentage of foreign flagged ships that arrive at US ports every year.

Having acquired a ship to execute an attack, terrorists may detonate explosives on the ship at a time or location of their choice, or ram the ship into the target. They may use surface-to-surface missiles to hit their target. Detonating explosives on an LNG tanker would be deadly. Richard Clarke, America's top counterterrorism official during 9/11, made the following comment about the Boston incident "Had one of the giant tankers blown up…, it would have wiped out downtown Boston." He further noted that the explosion of an LNG tanker would be as destructive as a nuclear bomb. Success in a scenario where a group of terrorists take over the control of a vessel with hazardous cargo and then launch an attack is less likely than in a scenario with a stowaway blowing up a foreign flagged vessel, as the Coast Guard could probably recognize the threat when they make an attempt to board the vessel. On the other hand, piracy may itself be easier than smuggling humans on a foreign flagged ship.

Bulk shipments of other hazardous cargo should also cause concern. In particular, ships carrying bulk shipments of ammonium nitrate are potentially vulnerable to terrorist attacks. In a Organization for Economic Co-operation and Development (OECD) Maritime Transport Committee report[123], explosive characteristics of ammonium nitrate is described as follows:

> *Ammonium nitrate is widely used throughout the world as an agricultural fertilizer and is generally considered a safe and stable compound when stored and handled correctly. However, with some manipulation (e.g. through addition of fuel oil) and triggered by a sufficiently large explosive catalyst, fertilizer grade ammonium nitrate can be used as a powerful explosive. Terrorist organizations throughout the world have been known to use adulterated nitrogen fertilizers to make powerful explosives (e.g. the truck bombings in Bali, Nairobi, Mombassa, Oklahoma City as well the first World Trade Center attack) prompting many countries to ban import of ammonium nitrate. The scale of potential destruction by a ship load of ammonium nitrate is several orders of magnitude greater than these truck bombs as can be seen from the 1947 Texas City explosion or the recent massive ammonium nitrate explosion in AZF plant in Toulouse, France.*

A huge volume of ammonium nitrate flows through inland waterways every year. For example, in 1997 over 400,000 tonnes of of ammonium nitrate was shipped through Mississippi river.[124] These shipments pass near urban centers such as New Orleans, St. Louis, Memphis, and Pittsburgh. In order to monitor and reduce vulnerability against ammonium nitrate and other hazardous cargo shipmens (commonly called certain dangers cargo or CDC), the Coast Guard acted to introduce new regulations in July 2004.[125] These regulations include mandatory development of security plans at vessels and facilities handling ammonium nitrate, preparation of vessel maintenance and security records, training of a facility and vessel security officer and installation of vessel and facility security systems. These new regulations increased the transportation cost of ammonium nitrate.

Inland waterways are vulnerable to attacks that could cripple freight routes and devastate waterfront cities, power plants, chemical facilities, and other ciritical and commercial targets. Some of the measures to address the terrorism threat in inland waterways include routine anti-terrorism patrols, establishment of maritime security zones covered with AIS technology, increased inspections on domestic tankers, and technology based surveillance around inland ports and critical facilities. The Coast Guard partnered with the

[123] OECD Maritime Transport Committee Report, "Security in Maritime Transport: Risk Factors and Economic Impact", July 2003.
[124] Ibid.
[125] Eddie Funderburg, "Is there a Future for Ammonium Nitrate?", www.noble.org, December 2004.

private sector to analyze the consequences of explosions on inland barges carrying CDC.[126] Since 9/11, inland ports are closed to foreign vessels.[127] The threat posed by barges and small watercraft is still present despite the positive security improvements made so far. Large segments of inland waterways still do not have any AIS coverage which increases the difficulty of surveillance.[128] For instance, "chemical barges that move up and down America's inland waterways are unmonitored".[129] There is an urgency to expand AIS coverage as soon as possible along inland waterways to reduce waterborne threat in America's heartland.

The risk of suicidal attacks on coastal targets from sea shores can be mitigated by blocking access from the see. Waterborne security barriers such as chains will prevent terrorists from either ramming into the facility or exploding bombs in the vicinity. Surface-to-air missiles can be utilized to counter surface-to-surface missile attack. However, we need remote sensor technology at maritime ports, power plants or other coastal targets to detect these attacks in advance. In particular, sensors that can detect nuclear content from distance could be a very valuable addition to nation's anti-terror armor. One challenge about implementing security measures is allocating the costs of alternative countermeasures among stakeholders.

DHS releases a National Infrastructure Protection Plan (NIPP) every year to coordinate a national effort that brings stakeholders in various sectors together and seeks to develop risk based framework for protecting critical infrastructure. Under this evolving plan, each economic sector has a Sector-Specific Agency (SSA) that develops, implements and maintains a Sector-Specific Plan (SSP) for protecting infrastructure within the sector. Various government bodies and private sector provide input into the plan to enhance comparative risk assessments within each sector. The goal is to prioritize certain assets in each sector and deploy limited resources accordingly to achieve maximum reduction in national terrorism risk exposure. SSAs are also responsible for threat assessments and identifying appropriate information sharing protocols that will facilitate vulnerability assessments by the private sector. For example, the Coast Guard is the SSA in port security, and as mentioned earlier, has finished risk assessments at nation's most critical 55 ports. According to recent GAO report, the Coast Guard has made progress in evaluating individual threats, degree of vulnerability and potential consequences of a terrorist attack. However, comparative risk assessments that are key to prioritize assets in funding decisions are not complete.[130] While NIPP includes all the necessary elements of risk based decision making for infrastructure protection, the benefits of such a comprehensive plan will be realized once DHS maps the national risk profile that enables comparisons across various sectors.

II. Pleasure and Fisher Boats

As mentioned earlier, tracking of general cargo vessels less than 300 gross tons is relatively poor as these vessels provide minimal information about their route. Since most fisher boats are under 300 gross ton requirement, there is no way of gathering intelligence about routes fisher boats take in fisheries. One scenario would be the transfer of illegal weapons or explosives in the open sea from a second vessel sailing in US waters. Another point of concern is that fisher boats permitted to enter the port area, which could let them launch an attack on critical targets in and around a seaport. Likewise, other open targets on the coast are vulnerable. A similar threat is posed by pleasure boats. Without further intelligence that triggers boarding of a specific boat, there is a little chance of intercepting terrorists.

[126] Statement of Rear Admiral Craig E. Bone on chemical facility security before the Homeland Security and Governmental Affairs Committee, 27 July 2005.
[127] Tim Jones, "US Heightens Vigilance to Protect the Mississippi", Chicago Tribune, 12 April 2003.
[128] "Federal Agencies Tackle Maritime Security, Ports First", National Defense, June 2005.
[129] Stephen Flynn, "Why America is Still an Easy Target.", Time, 26 July 2004.
[130] GAO Report, GAO-06-91,"Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure", 15 December 2005.

Drug smugglers are known introduce illegal drugs on fisher boats for a long time. As the threat of terrorism intensifies, fisher boats may be a new means to introduce explosives or weapons in the homeland. Most marinas have minimal protection from terrorists. Thus, as long as a fisher boat escapes the Coast Guard's notice, success is very likely. According to GAO, resource hours allocated to drug interdiction has reduced 44%.[131] However, drug interdiction performance did not reflect this reduction on hours devoted to the mission. The Coast Guard attributes this to improved efficiency in operations due to new technology. Recent evidence of increased criminal activity involving drug cartels beyond the southwestern land borders may suggest that this could be attributed to increased drug traffic. In one senate hearing, Michael O'Hanlon of Brookings Institution said:[132]

> *In the immediate aftermath of 9/11, more than half of the Coast Guard was devoted to port and waterway security against possible terrorist attacks. Even today, at least a quarter of Coast Guard assets are devoted to such missions. Other activities ranging from environmental protection to patrolling of US economic maritime zones to counterdrug missions have suffered.*

Reduction of hours devoted to drug interdiction may have negative impacts on weapons interdiction. Increased rate of random boat inspections may be an effective deterrence based solution to the problem. Expansion of initiatives and technology investments increasing maritime domain awareness to include intelligence gathering on fisher and pleasure boats would be another effective risk mitigation effort.

III. Waterways and Underwater Security

Most of the discussion which is relevant to waterways security is already provided in previous sections as there is a significant overlap between waterways security and security of coastal targets. What distinguishes waterways security from the other two sub-components is the threat on commercial traffic flowing in US waterways. Coordinated suicide attacks on ships carrying hazardous or other commercial cargo and mine attacks are the most prominent scenarios that target economic prosperity by disrupting trade. Increased maritime domain awareness that could help the Coast Guard observe, report and respond to suspect activities of vessels will mitigate both risks. Vessels should develop anti-piracy measures to detect any suspicious activity around and report valuable information that could help early response.

Terrorists may choose to disrupt the trade by laying mines in a port, or around critical waterways. If mines hit a ship with hazardous cargo, then the damage can be compounded. Terrorists may lay mines by vessels or frogmen. This threat raises questions about underwater security, which has been overlooked in the past. A countermeasure to this threat would be to equip the Coast Guard vessels with mine sensors. No extra resource hours would be allocated for this mine search mission as regular patrolling activities would accomplish the task. The Coast Guard is aware of the problem and unveiled an integrated anti-swimmer (IAS) system to address this threat.[133] The system integrates technology with human monitoring. Underwater and sonar cameras are used for continuous monitoring, whereas swimmers and divers can be used to thwart underwater bombers. Underwater weapons called as "nonlethal interdiction acoustic impulse" devices were still in testing phase earlier in 2005.[134] The Coast Guard plans to use these weapons after a verbal warning using underwater speaker systems. These countermeasures are to deter frogmen

[131] GAO Testimony, GAO-04-636T,"Coast Guard: Key Management and Budget Challenges For Fiscal Year 2005 and Beyond", 7 April 2004.
[132] Senate Governmental Affairs Committee Hearing, 20 March 2003.
[133] "USCG Unveils 'anti-swimmer' System to Thwart Underwater Terror Attacks", Emergency Preparedness News, 22 March 2005.
[134] Eric Lipton, "Coast Guard Turns Its Eyes Underwater", New York Times, 2 February 2005.

from laying mines around ports, rather than mine detection and sweeping. The US Navy has resources for mine sweeping and detection activities. However, some of these resources are currently deployed for overseas operations. Furthermore, all of the resources (Coastal Mine Hunters and Mine Countermeasures Ships) available domestically are based in Texas. This increases vulnerability to a mine attack at certain locations in US waterways as it may be difficult to deploy minesweepers on time. In particular, any West Coast port will gave particular vulnerability as it may take a month for a minesweeper to cross Panama Canal and arrive at the port under attack. It is mandatory to have highly trained divers at or sufficiently close to critical locations who can clear mines in the case of an attack.

The Coast Guard should be vigilant against distraction scenarios. A terrorist group seeking to sneak through a relatively well protected portion of the maritime borders may place a rescue call to the Coast Guard, and then send boats full of illegal weapons and explosives while the Coast Guard is busy conducting rescue operations. This scenario will likely succeed in regions where the Coast Guard is relatively undermanned and underequipped. The Coast Guard should be able to maintain a fleet size that would enable multiple operations simultaneously to minimize the threat of a distraction scenario.

IV. TERRORISM THREATS AND VULNERABILITIES ALONG LAND BORDERS

The United States has a long history of confronting illegal aliens or drug smugglers seeking to cross borders. As the threat of domestic terrorism intensified, there is a renewed urgency to protect the land borders from terrorist traffic. Two main agencies under DHS are responsible from securing land borders. CBP assumes majority of the law enforcement functions along land borders. It is responsible from keeping terrorists and illegal weapons from entering US, and thus faces the challenge of patrolling and protecting an enormously wide area along US land borders. On the other hand, ICE assumes investigative functions. ICE is responsible from detecting and preventing terrorist acts, and hence from interior law enforcement. ICE functions are related to land border security as the failure of a land border component does not necessarily imply a terrorist attack. The success probability of a terrorist attack depends also on the interior enforcement activities of ICE.

The United States shares a 3,987[135] miles (3,145 miles on land) border with Canada and 1,951[136] miles border with Mexico, with a combined total of 115 land ports of entry, 84 of which is on Canadian border. Prevention of illegal entries is a huge undertaking given limited resources and vast stretches of virtually uninhabited land. Unlike maritime borders, land borders are not likely to be targets themselves. This does not reduce the threat along land borders as relative ease in crossing land borders may attract terrorists with nefarious plans to attack inland targets.

A. Threats along Land Borders

Threats along land borders come mainly from smuggling networks that could help illicit importation of weapons and illegal alien traffic. They may be realized as unimpeded border crossing between ports of entry or undetected cargo crossing at land ports of entry. Drug cartels and human smugglers have used similar avenues and developed the expertise that terrorists may use to cross borders. Therefore, performance of CBP officials in their efforts to interdict illegal crossings and smuggling attempts for other criminal purposes may be an indicator of how successful they could be in interdicting terrorists.

1. Recent History of Illegal Crossings

Historically, land borders have been porous. Prior to 9/11, the main threat was posed by illegal aliens, smugglers of drug and other contraband and other potential criminals. However, the persistence and commitment of terrorists to execute attacks in the American Homeland has shifted attention to inadequately defended southwestern and largely undefended northern land borders. Canadian border was traditionally quoted as the “World’s longest undefended border”[137]. There is no evidence that any of the terrorists who participated in 9/11 entered illegally crossing borders. In fact, most of them had legal visas. There have been only two confirmed attempts to illegally cross the border for terrorism purposes. Abu Maizar, a Palestinian from West Bank, was caught crossing the northern border with charges of conspiracy to blow up New York subway station in 1997. He was reported to have made two earlier attempts to sneak into Washington State from Canada, each of which resulted in his arrest and return back to Canadian officials.[138] The second incident was the arrest of Algerian national Ahmed Ressam driving off the ferry from Canada to Port Angeles of Washington state.[139]

[135] Source: International Boundary Commission website, www.internationalboundarycommission.org.

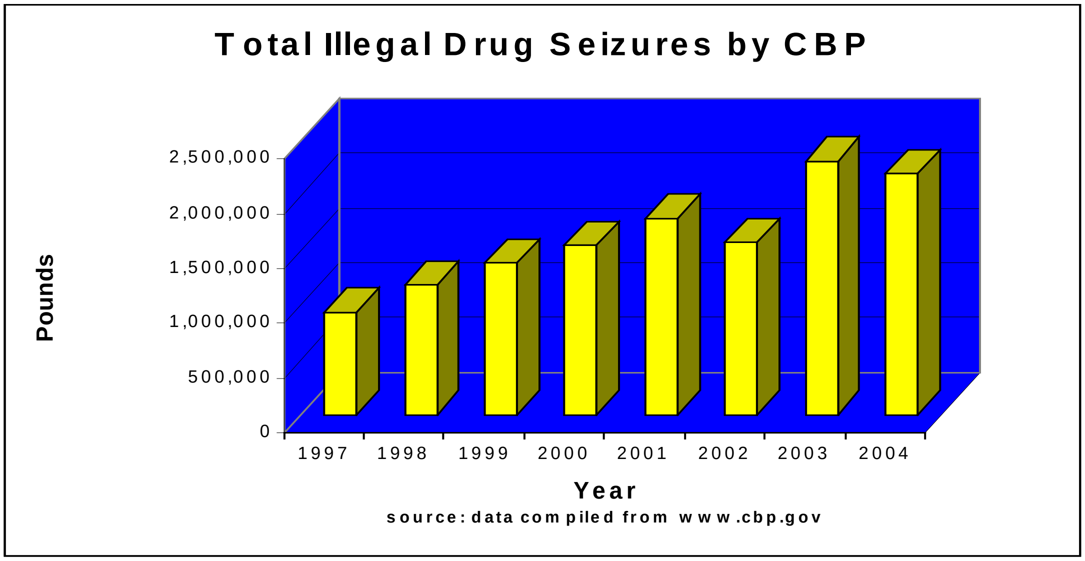
[136] Source: Embassy of Mexico website: http://portal.sre.gob.mx/usa/.

[137] See the article “Danger at Our Door” by Doug Most at www.bostonmagazine.com and NPR special report “Strangers at the Gates” at www.npr.com.

[138] Dan Barry, “Bomb Suspect was Detained by US But Released”, The New York Times, 2 August 1997.

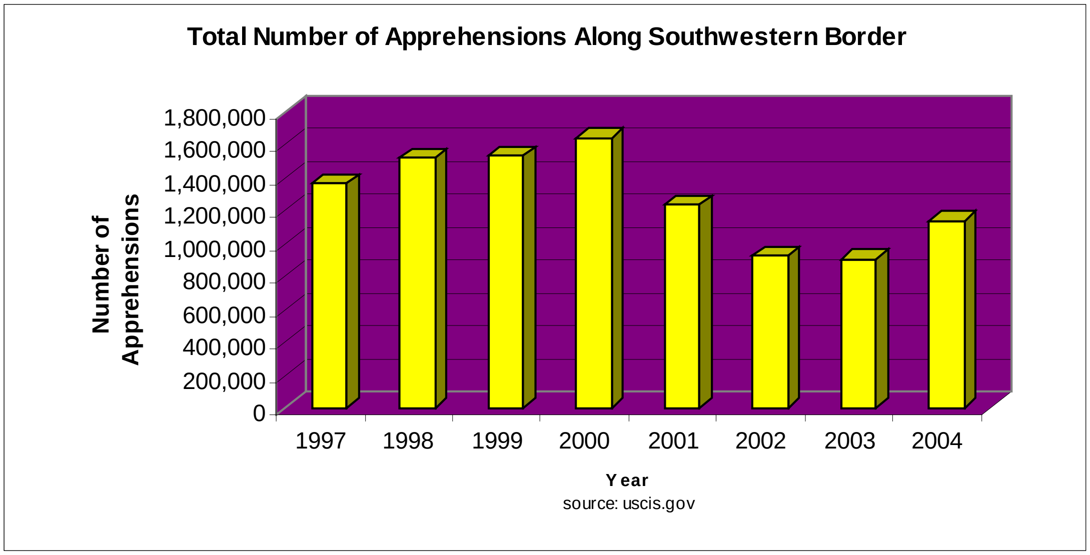
[139] Sam Howe Verhovek and Tim Weiner, “Man Seized with Bomb Parts at Border Spurs US Inquiry”, The New York

Figure 12



source: data compiled from www.cbp.gov

Figure 13



source: uscis.gov

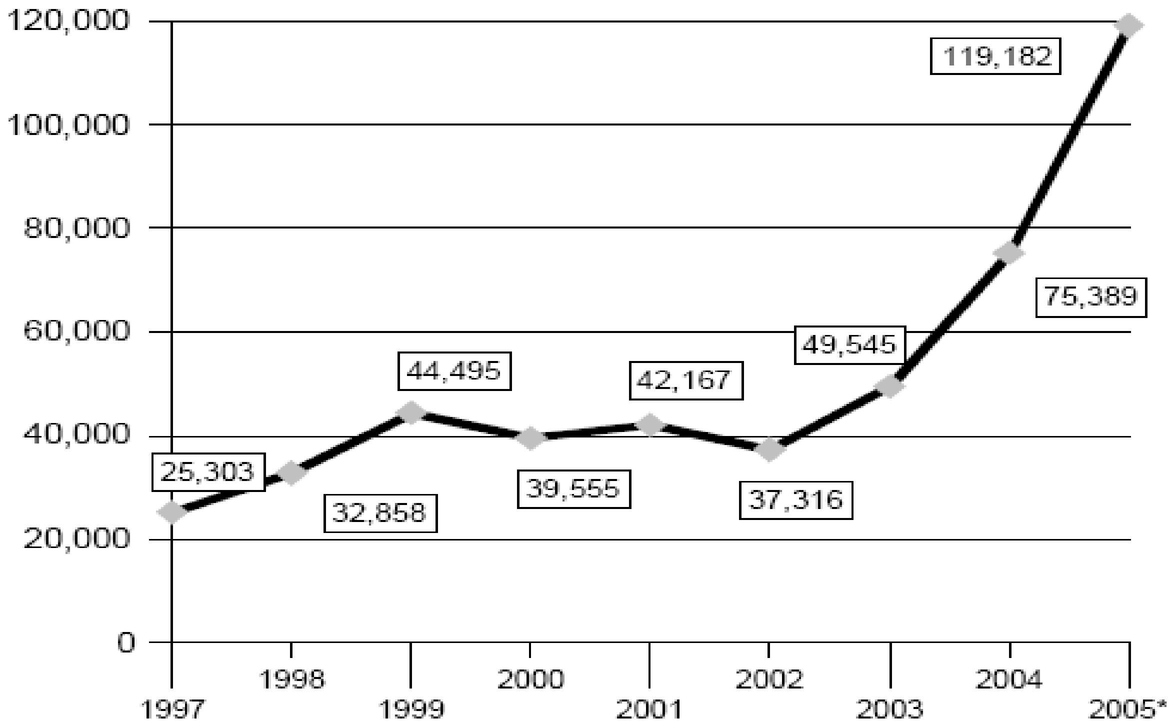
Drug smuggling volume has consistently been on the rise. Figure 12 illustrates this rising pattern. A vast majority of seizures during FY ’97-’04 period have been marijuana whereas smaller volumes of cocaine, heroin and khat have also been seized. There is a minor decline in 2002, partially due to increasing awareness of the problem right after 9/11, however, statistics and recent incidents beyond the southwestern border suggest that numbers may be picking up. In the first six months of 2005, more than 600 were killed in Mexico due to drug cartel violence.[140] This suggests that despite measures taken to deter illegal

Times, 18 December 1999.

[140] Marla Dickerson, “Mexican City Pays the Price as Drug Gangs Fight for Territory”, Los Angeles Times, 7 July 2005.

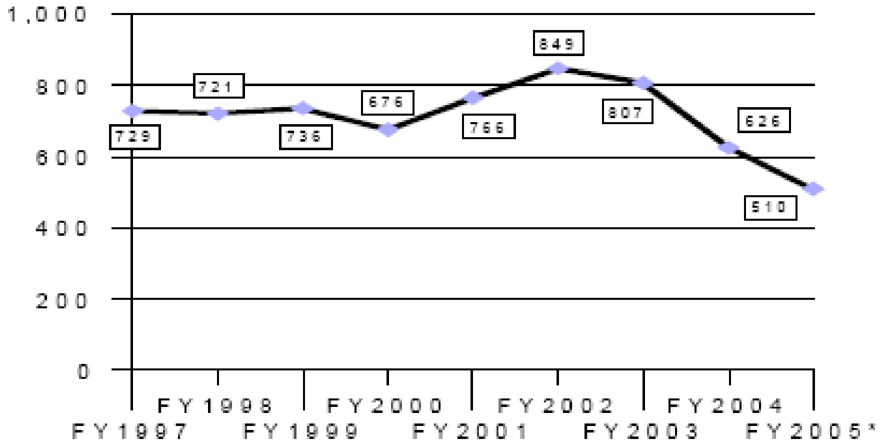
crossings, drug smuggling is still a lucrative business and drug cartels will remain active in years to come.

Figure 14 OTM Apprehensions by Fiscal Year[141]



*FY2005 Data Through July 11

Figure 15 Special Interest OTM Apprehensions[142]



* FY2005 data through July 11

Illegal alien apprehensions, on the other hand, have declined after 9/11. The number of apprehensions climbed up to over 1.6 million in 2000, however, due to increased surveillance, border patrolling and slowing

[141] Source: CRS Report for Congress, “Border Security: Apprehensions of 'Other Than Mexican' Aliens”, 22 September 2005.
[142] Ibid.

economy, the number was kept below one million in 2002 and 2003. This slowing trend may come to an end in 2005 as the traffic flow has increased to an extent that required state of emergency declaration from governors of both New Mexico and Arizona in the summer.[143] While the vast majority of illegal aliens apprehended were Mexican nationals, people from Central America, South America and the Middle East also contributed to this figure. Apprehension statistics at the US-Mexico border for those classified as Other Than Mexican (OTM) are given in Figure 14. There is a clear increasing trend of OTM crossings. However, this increasing trend is not observed for crossings of "special interest"[144] countries. Figure 15 demonstrates that there is an approximately 40% decrease in "special interest" apprehensions.

There is no exact way to determine the number of illegal aliens. However, a good estimation of this figure is crucial for assessing the probability of a successful illegal entry through borders. In December 2003, then-Homeland Security Secretary Tom Ridge estimated the number to be between 8-12 million.[145] This educated guess is probably based on the US Census Bureau's 2000 estimate of 8,705,419 illegal immigrants based on residual foreign born method.[146] Given the 1990 estimate of 3,765,906 [90], the rate of increase in the number of illegal aliens is roughly 500,000 per year in '90's. These estimates may be very conservative. In a letter by Senator John McCain (R-AZ) in February 2004, Senator claims "According to the US Border Patrol apprehension statistics, it is estimated that almost four million people crossed our borders illegally 2002."[147] Furthermore, "it is widely accepted that a similar number crossed our borders illegally the previous year, 2001".[148] In a senate hearing on June 17, 2004, Republican Congressman Jim Kolbe (R-AZ) responded to a question by Senator John McCain stating that only "one out of four or five" illegal immigrants were apprehended in the previous year.[149] According to one study at Northeastern University, the actual number can be as high as 13 million in 2001.[150] There are even estimates that "a minimum of 20 million illegal aliens are presently residing in the United States, with an average of 12,000 illegal aliens entering every day".[151]

Terrorists and weapon smugglers have historically been undeterred by harsh environmental conditions of relatively undefended borders. They "respect no boundaries and no set of laws".[152] Osama Bin Laden is still believed to be on the move between mountainous Afghanistan and Pakistan border.[153] Armed guerillas have been present in between Central Asian nations of Kyrgyzstan, Tajikistan and Uzbekistan in '90s.[154] PKK, a terrorist group that engaged in a 16 year war with Turkey, used the Iraq and Syria as a base for their operations, crossing the relatively undefended southeastern border at will. They still have base camps in northern Iraq, and occasionally clash with American troops in the region.[155] Thus, cross-border terrorism

[143] "Law and Border", Los Angeles Times, 18 August 2005.
[144] Potential future terrorists are believed in the intelligence community to originate from one of these countries of "special interest".
[145] Jerry Seper, "Ridge Rapped for Immigration Views", Washington Times, 11 December 2003.
[146] US Census Bureau website: www.census.gov.
[147] www.desertinvasion.us.
[148] D.A. King, "Could There Be Twenty Million Illegals In the US?", The American Resistance (www.theamericanresistence.com), 7 August 2004.
[149] Lou Dobbs Tonight on CNN, 17 June 2004. The recording of this program can be found at www.americanpatrol.com.
[150] "Feds Undercount Illegal Aliens", www.newsmax.com, 16 March 2001.
[151] "How Many Illegal Aliens are in the US?", www.theamericanresistence.com, 3 January 2005
[152] Ambassador Cofer Black, Coordinator for Counterterrorism, "The Prevention and Combating of Terrorism in Africa.", Remarks at the Second Intergovernmental High-Level Meeting on the Prevention and Combating of Terrorism In Africa, www.state.gov, 13 October 2004.
[153] Henry Schuster, "Where's Osama?", www.cnn.com, 26 April 2005.
[154] Paula R. Newberg, "Terrorism: Spreading Chaos in Central Asia.", Los Angeles Times, 19 September 1999.
[155] "US Troops Clash with 'PKK Rebels'", BBC News, 10 November 2003.

has also created regional problems elsewhere and threatened the world peace.

2. Motives for Illegal Border Crossing for Economic Migrants

Majority of economic migrants do not pose any terrorism threat to United States. However, illegal crossings of economic migrants are an important part of the equation for two reasons. First, the Border Patrol and other law enforcement agencies have to allocate valuable resource hours that could otherwise be directed to minimizing terrorism threat along the land borders. Second, terrorists can potentially blend with economic migrants crossing the border and exploit similar vulnerabilities to achieve their terrorism goals.

Statistics provided in the previous section suggests that the number of illegal aliens crossing borders in a given year is increasing, despite measures taken to beef up security along land borders. The slowing economy in the beginning of the new millennium helped reduce the numbers as expectations of employment presumably faded. However, the president's proposal of a temporary worker program in January 2004 increased the hope of finding a job in the United States and eventually gaining permanent residence. The bill that which was introduced last May to this end seeks to initiate a new temporary visa program.[156] Recently Homeland Security Secretary Michael Chertoff outlined Bush's plan to implement the program.[157] Under the president's plan, the guest workers will be permitted to stay for three years, and will be asked to return to their home country at the end of this period. They will also be given the option to extend their permit for a second three year period. Biometric, tamper-resistant cards will be used for their border crossings. The goal is to fill jobs that the Americans are not willing to take.

However, according to many Americans who already feel the risk of losing jobs, this program will simply provide further incentives for companies to offer unacceptably low wages to attract illegal aliens and thus reduce labor costs. Currently, illegal immigration costs annually $133 billion in job losses, $68 billion in providing benefits and $7 billion in welfare for medical assistance.[158] Some industries are believed to employ a good number of illegal aliens, although it is illegal to do so. The Immigration and Naturalization Service (INS) has not gone forward to enforce the law in most cases. For instance, in 2002, only 13 employers nationwide were levied fines for the practice of employing illegal aliens, which is believed to be an insignificant number compared to thousands of potential employers continuing the same practice.[159] Tom Doheny, the president of the US Chamber of Commerce, believes that the need to legalization of illegal workers in the United States is desperate as he said[160]

> *If we could stop it right now, take those 12 million people and send them home, the hotels, the hospitals, the nursing homes, the agriculture business and many of the factories in this country would be seriously short staffed and in the public service, areas of medical and care of elderly would be in absolute crisis.*

His statement gives us a clue about how much the US economy depends on illegal aliens. Since the American manufacturers are facing a very tight competition with the overseas producers, the need for lowering labor costs becomes a matter of survival for most companies. However, this program may be exploited by terrorists to legalize themselves and conduct their operations more safely.

The poverty level in Mexico and the prospects of having a better way of life in the United States is the main

[156] "Major Immigration Surgery", The New York Times, 20 May 2005.
[157] "Chertoff, Chao Promote Guest Worker Program", www.cnn.com, 18 October 2005.
[158] Bill Hess, "Military's Use on the Border Expands", Sierra Vista Herald, 21 April 2005.
[159] Donald L. Barlett and James B. Steele, "Who Left the Door Open?". Time, 20 September 2004.
[160] NPR Special Report: Strangers at the gates, January 2002.

motivating factor for the influx of millions of illegal aliens. Many illegal aliens are willing to risk their lives during their painful journey into the United States. Coyotes are providing a service for illegal immigrants for a fee.[161] There does not seem to be any measure to deter illegal aliens from crossing the borders other than dangerous terrain itself. The ones that are apprehended are not subject to prosecution by US officials unless they already have criminal records in US, and are simply deported back to Mexico. Many of them come back and try once again. Mexican illegal aliens can get multiple "free" border crossing attempts before they face any prosecution.

3. Possible Links between Terrorists and Illegal Aliens

Terrorists' agenda does not include getting jobs in the United States, so one might question the nexus between the illegal alien issue and homeland security. A good number of criminals are apprehended along the southwestern border every year. For instance, from October 1, 2003 to July 20, 2004, 9051 persons with criminal records in US were apprehended in Tucson sector. The number of illegal aliens with criminal records apprehended since President Bush has taken office exceeded 350,000.[162] We have to note that such statistics do not include those who have committed crimes in Mexico, as this information is not available to the US Border Patrol. These criminals, as well as the coyotes on Mexican side of the border may be easily persuaded to help terrorists to cross borders. In addition to those aliens from potentially rogue states captured along national borders, the US Border Patrol recently apprehended a Bangladesh citizen crossing through a wooded area in south Texas.[163] He was accompanied by 13 other undocumented aliens, one of which was later identified as a member of Mara Salvatruchas, a local street gang known in a variety of criminal activities such as burglaries, auto thefts, narcotic sales, home robberies, weapons smuggling, car jacking, extortion, murder, rape, witness intimidation, illegal firearm sales, car theft and other aggravated assaults.[164] On this alleged link between Mara Salvatrucha and Al Qaeda, Congressman Solomon P. Ortiz (D-TX) said "We knew this was happening underground, but now it's come to the surface." In an earlier incident, a would-be terrorist linked to 9/11 attacks were apprehended at the Texas-Mexico border in 2003.[165]

Al-Zarqawi, who is believed to lead a terrorist group responsible from beheading of its captives, attacks on US forces and Iraqi security forces, is reportedly planning assaults in the United States after penetrating through the Mexican border.[166] According to a restricted bulletin prepared by US security agencies, Al-Zarqawi believes that the best way to penetrate in the United States would be obtaining a visa to Honduras and then moving through Guatemala and Mexico before using an open spot along the southwestern border. This scenario was further corroborated by the earlier reports of a top Al-Qaeda lieutenant meeting Mara Salvatrucha gang members in Honduras.[167] If Al-Zarqawi's terrorist network ever finds a chance to land people in Honduras, crossing Central America's borders won't be a big problem. Many Central Americans heading to the United States are already crossing the borders in Central America facing minimal deterrence. Horacio Schroeder Bejarano, public security secretary of Mexico's Chiapas state on Guatemala border recently said "We have a very porous border, and it is very vulnerable."[168]

[161] According to the NPR's special report, this fee ranges between $600 to $1200 per trip across Arizona border.

[162] These statistics were quoted by President Bush when he gave a speech at Davis-Monthan Air Force Base on his immigration reform proposal. November 28, 2005.

[163] Sergio Chapa, "Bangladeshi's Arrest Prompts Concern over Border Security", The Brownsville Herald, 10 December 2004.

[164] Al Valdez, "Mara Salvatrucha Street Gang", www.freerepublic.com, 31 October 2004.

[165] Ed Gordon, "Undocumented Workers", NPR, 5 April 2005.

[166] Adam Zagorin, Timothy J. Burger and Brian Bennett, "Zarqawi Planning a US Hit?", Time, 21 March 2005.

[167] Jerry Seper, "Al Qaeda Seeks Tie to Local Gangs", The Washington Times, 28 September 2004.

[168] Chris Kraul, "A Surge South of Mexico", Los Angeles Times, 1 May 2005.

The Canadian Security Intelligence Service identified 50 terrorist groups active within Canada in 2000.[169] Threat from northern borders originates mainly from Canadian immigration policy. Immigration policy of Canada has been open to foreign nationals in the past who have shown some quality educational background and relatively good skills in English or French. Canada is a country with ten states, nine of which follow similar immigration policies and procedures, excluding Quebec. The state of Quebec has its own immigration policy and procedures, which has been quoted as "separate and more liberalized than Canadian immigration policy."[170] According to Canadian Integrated National Security Assessment Center's report, a number of alleged jihadist sympathizers are citizens of Canada.[171] Canadian immigration and asylum policies have been described as "lax and generous", accordingly "inviting terrorists to use Canada as a back office for fund raising, document forgery and planning". In particular, Quebec has been accused for its "efforts to attract French speaking immigrants, including many from North Africa" as it is argued that "these efforts have unwittingly helped create an ethnic backdrop in Montreal that makes it easier for Islamist radicals from countries such as Algeria to blend in."

Last February, an Algerian-Canadian terrorist, Fateh Kemal returned to Montreal having been released from a French prison for terrorist crimes.[172] We have to realize that most Arabic speaking Middle Eastern countries have been a French colony. Thus, the educational curriculum is designed to give each student a good command of French language. An immigration applicant from those countries can get a good score on language proficiency, which increases the chances of admission. Besides, both of the known historical attempts to cross borders for launching attacks in the United States have been recorded in the north. Threats posed from the northern border may not be any less than from that of southwestern border. A terrorist from Canada would have a clear advantage at the moment to sneak illegal weapons and other contraband into this country as he needs to provide minimal documentation. A disproportionate allocation of resources could simply be an open invitation to terrorists to use poorly defended sections of US land borders.

B. Vulnerabilities along Land Borders and Countermeasures for Risk Mitigation

We analyze the vulnerabilities along the entire land borders under two categories: ports of entry and between ports of entry. Border security enforcement is the responsibility of Bureau Customs and Border Protection (CBP) under DHS which was created by merging Department of Justice's Immigration and Naturalization Service (INS) and the Department of Treasury's Customs Service. Majority of the travelers cross land ports of entry by personal vehicles, whereas a smaller percentage chooses to cross on foot or by bus. Individuals seeking entry into the United States are inspected at the ports of entry by CBP officials most of which were formerly with the US Customs, INS and the Animal Plant Inspection Service. Between land ports of entry, the US Border Patrol holds the operational control of national land borders.

1. Land Ports of Entry

Land ports of entry are facing a relatively balanced traffic load of both people and cargo moving across. While the focus is more on people for aviation security and more on cargo for maritime security, both people

[169] Christopher J. Chipello and Dan Bilefsky, "A Global Journal Report: Is Canada a Launching Pad for Terror?—Montreal In Particular Offers Camouflage for Operatives Plotting Far-flung Assaults", The Wall Street Journal, 10 July 2002.

[170] These comments were made by an Indian lawyer, Prashnant Ajmera, currently working as a licensed immigration consultant in Canada since 1993.

[171] Stewart Bell, "Influx of Terrorists", National Post, 9 May 2005.

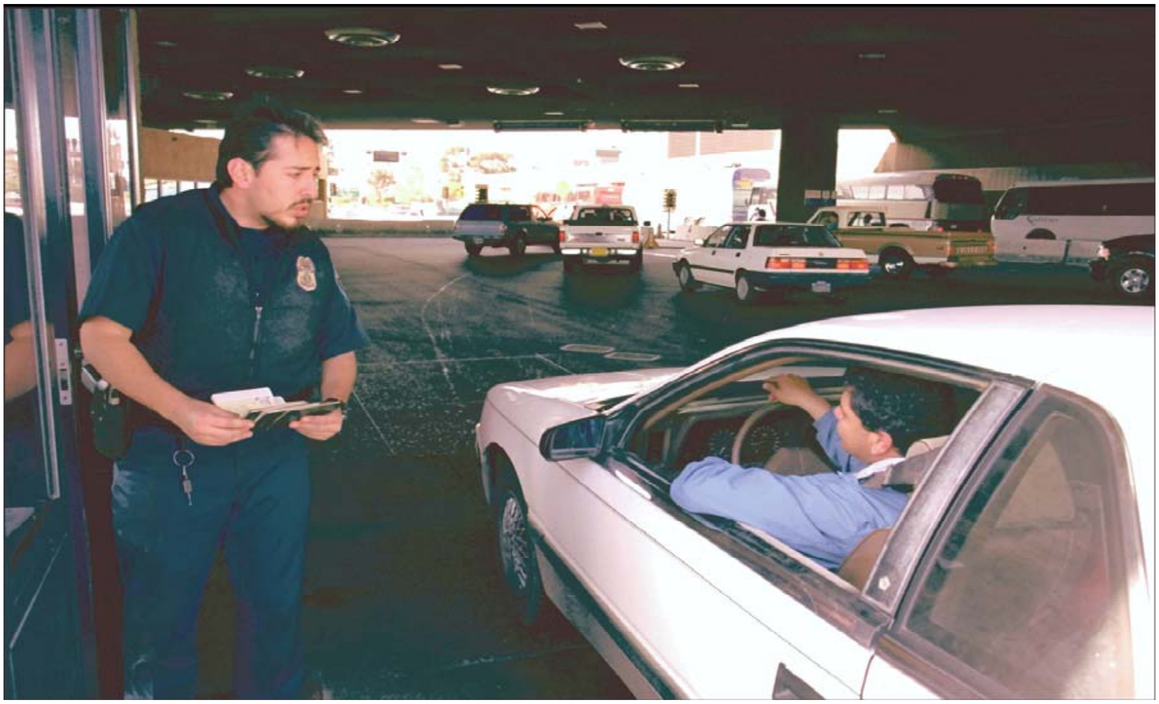
[172] "Canada: Terrorist Returns; Conservative Party Leader Urges Ottawa to Consider not Playing the Dhimmi", www.jihadwatch.org, 27 February 2005.

and cargo deserve the same level of attention for land borders. In this section, we discuss vulnerabilities on two final sub-components under land ports of entry. Most procedures on both side of the borders are the same, however admission procedures of Canadian and Mexican citizens have differences. As far as cargo is concerned, procedures and operational restrictions for truck crossings and level of resources deployed mark the difference between the north and the southwest.

a. People Crossing Ports of Entry

Legal entry to the United States through ports of entry requires resolve of two issues. First, the traveler has to prove that he is either a US citizen, or an alien entitled to stay in the United States. Second, the inspector must confirm that the traveler is not engaged in smuggling of drugs, weapons or other contraband. The primary inspection is rather rapid as the inspector asks several questions about the status of the traveler in US, purpose of the visit, his nationality and reviews the travel documents that are required for admission. If the traveler does not readily meet the requirements for admissibility, secondary inspection procedure is implemented. In 2002, 9 million out of 453 million inspections resulted in this second more intensive phase.[173]

Figure 16 Driver Being Questioned during the First Phase of Inspection. Source: GAO-03-174



It is the secondary inspection phase that dramatically increases the chances of interception of a terrorist, smuggler or an illegal alien. The traveler's belongings and car goes through a detailed examination, required documents are reviewed with higher scrutiny to verify identity and the traveler is questioned more thoroughly. Identity check is performed using biometrics under the US-VISIT program currently at the busiest 50 ports of entry.[174] Digital and inkless fingerscans taken at the port of entry is matched with the traveler's fingerscan taken when the visa is issued. The inspector can digitally view photographs taken

[173] GAO Report, GAO-03-1084R, "Land Border Ports of Entry: Vulnerabilities and Inefficiencies in the Inspections Process.", 18 August 2003.
[174] Fact Sheet: US-Mexico Land Borders, Department of Homeland Security website www.dhs.gov

during the visa interview. Biometric information is also checked against watch lists. DHS's goal is to implement US-VISIT in the secondary inspection areas of all the remaining ports of entry by December 31, 2005.

After the second inspection phase, the inspector may deny entry, in which case the alien may be subject to penalty, including arrest if the alien is a criminal on the watch list. However, the law gives the right of withdrawing application for the alien, which permits the alien to reapply for entry in the future without penalty. Prior to 9/11, over 60% of the withdrawal requests were accepted. However, this figure dropped to 37% in fiscal year 2001 and 34% in fiscal year 2002.[175] The inspector allows withdrawals if violation is not serious, the alien does not have a clear intention to violate the law and does not have a long history of similar violations.

Vulnerabilities during the first phase are related with probability of false admission, whereas in the secondary phase, concerns are more in terms of costs of implementing an intensive inspection.

A potential terrorist seeking to introduce weapons or explosives can be successful if he can evade the secondary inspection phase. The effectiveness of the first phase mainly depends on the training and the experience of the customs official and the ability to ask "smart" questions to the traveler to identify if the stated purpose to enter the country does not contradict the actual purpose. While inspectors have been able to identify terrorists during the first inspection phase in the two earlier confirmed attempts to enter US for adversarial purposes, we have to recognize that an error may result in a terrorist attack somewhere in the homeland.

The likelihood of error may not be as low as we think it is. Currently, American citizens are not required to present passports for land border crossings.[176] This raises the question of whether terrorists will be granted entry to the United States if the inspector is convinced that he's a US citizen. Randy Callahan, the Executive Vice President of National Homeland Security Council made the following comment about those who seek entry, "…right now, there's no requirement to have a US passport or a US documentation to come in from Mexico. So if he speaks good enough English and can convince the inspector that he's a US citizen, they'll let him through".[177]

Using the biometric technology reduces the likelihood of issuing a visa for a terrorist. Thus, most terrorists may avoid using land ports of entry to cross borders. However, this does not reduce the risk posed by possible introduction of illegal weapons through ports of entry. Terrorists may find people with appropriate documents who would cooperate by introducing illegal weapons such as MANPADS, rocket propelled grenades or sniper rifles through land ports of entry for some monetary compensation. These weapons can easily fit into trunk of a car or an SUV. A typical scenario would be to utilize such weapons to launch an attack to a flying aircraft from the airport perimeter. [178] There is an urgency to deploy screening technology at land ports of entry to minimize the likelihood of sneaking through with weapons and explosives. Utilization of such a technology may not cause long delays if all travelers and cars pass through relocatable X-ray devices. The secondary inspection can be performed on those who were not admitted based on the screening process as well.

[175] CRS Report to Congress, "Border Security: Inspections Practices, Policies and Issues", 26 May 2004.

[176] According a new Western Hemisphere Travel Initiative, US citizens will be required to present their passports by the end of 2007.

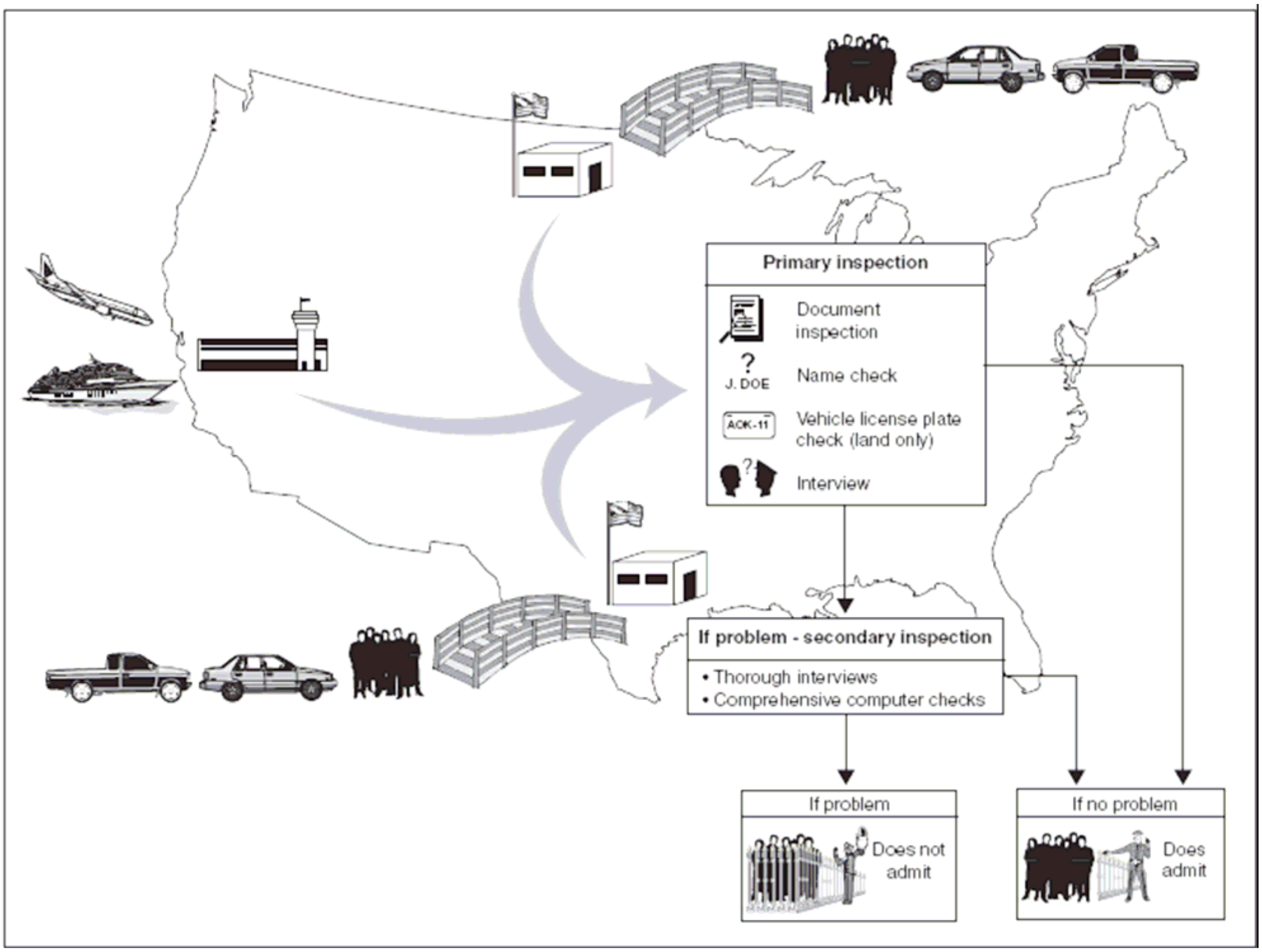
[177] Congressional Hearing before the Subcommittee on Immigration, Border Security and Claims, 10 March 2005.

[178] For an extensive discussion of threats posed by MANPADS and other ballistic weapons, please see Terry O'Sullivan, "External Terrorist Threats to Civilian Airliners: A Summary Risk Analysis of MANPADS, Other Ballistic Weapons Risks, Future Threats and Possible Countermeasures Policies", CREATE, 14 April 2005.

The documentary requirements are different for Mexican and Canadian nationals. Mexican nationals present a special visa for short term entries up to six months, which is good for at least ten years. Canadian nationals currently are not required to present passports, but by the end of 2005, all the Canadian nationals will be asked to present a passport to enter the United States. While none of global terrorist groups are known to have a sizable number of sympathizers in either Mexico or Canada, presence of local terrorist organizations in Canada raises concern.

Another challenge for the first phase is the training of inspectors. In a 2003 GAO testimony[179], two problems are pointed out. According to GAO, insufficient time is devoted to training due to pressures of inspection itself and many ports of entry have new inspectors who lack sufficient experience. This may undermine the capabilities to correctly identify those who smuggle weapons, explosives, drugs and other contraband. In the same report, some concerns were also raised about the ability of inspectors to process an enormous amount of intelligence information. This will increase risk of overlooking an important piece of information, further increasing the likelihood of a failure.

Figure 17 US Port of Entry Inspection Process. Source: GAO-03-174



[179] GAO Testimony, GAO-03-546T, “Border Security: Challenges in Implementing Border Technology”, 12 March 2003.

Concerns about the secondary phase are related to the US-VISIT program. While there are some potential technology related vulnerabilities[180], delays that might be caused by full implementation of the US-VISIT program is posing more repulsive challenges.[181] It is due to this drawback that travelers are not required to provide biometric information during the first phase. CBP seeks to alleviate congestion problems at the land ports of entry by implementing frequent traveler programs such as SENTRI (Secured Electronic Network for Travelers) and NEXUS. SENTRI system works by installing a transponder on the vehicles. The inspector compares pictures taken at the registration with pictures in the database and makes an admission decision based on a visual comparison. The average inspection time is reduced to 10 seconds from the earlier 30-40 seconds.[182] NEXUS works on a similar principle, using a proximity card that is issued to each registered traveler instead a transponder on a vehicle. However, both programs are implemented at a very limited number of ports of entry as the necessary technology and equipment have not yet been deployed.[183]

b. Cargo Crossing Ports of Entry

Cargo entering US on truck and rail poses risks to the homeland. Over 11 million trucks commercial trucks cross borders per year.[184] Customs inspected 22.6% of rail containers, 5.2% sea containers and 15.1% of trucks physically in fiscal year 2002.[185] As of February 2005, 164 large-scale NII systems have been deployed to ports of entry.[186] This figure includes all systems for maritime and land ports of entry. CBP is planning to build a database to keep advance cargo manifestation information. When this database is ready, all trucks and cargo trains will have to report their cargo information one hour prior to arriving at a port of entry. This regulation has been issued under the Trade Act of 2002. According to CBP Commissioner Robert Bonner, "We'll be able to do an advanced evaluation of risk in terms of those shipments before they arrive at our border, because right now they arrive sort of blind. We often don't know who the truck is, where it's coming from, what's supposed to be in it until it actually arrives at the port of entry."[187] Hence, CBP is currently not able to classify the incoming cargo based on the real level of risk they pose.

Currently, CBP implements Border Release Advanced Security Selectivity System (BRASS) that tracks highly repetitive shipments to ensure that cargo information on the bar code matches with information on the invoice. This system is designed to expedite shipments by keeping a track on trade activity across the border. However, it provides no security measure to verify that a shipment does not contain illegal weapons or explosives.

Free and Secure Trade (FAST) is a voluntary program expediting faster release of qualifying shipments from land ports of entry. This program seeks to ensure faster and more secure trade. Among benefits are

[180] GAO Testimony GAO-03-546T pointed out that a biometric technology database may not be able to hold all the identity information. DHS currently uses Automated Biometric Identification System (IDENT) to store all the identity information under US-VISIT. Another GAO report GAO-04-1080T raised concerns on the lack of guidance to consular posts on how and when to use information on IDENT.

[181] According to Brian C. Goebel of Gibson, Dunn & Crutcher LLP, even a minimum of 30 second delay caused by collection of biometric information will cause intolerable delays for the travelers crossing the border by car. He made this comment at the Transportation & Border Security Conference at Arlington, VA on 3 May 2005.

[182] GAO Report, GAO 03-174, "Technology Assessment: Using Biometrics for Border Security.", November 2002.

[183] For the list of ports of entry where SENTRI and NEXUS are implemented, visit http://apps.cbp.gov/bwt

[184] "Transforming Border Management in the Post September 11 World", Council on Foreign Relations, 18 January 2002.

[185] CRS Report to Congress, "Border Security: Inspections Practices, Policies and Issues", 26 May 2004.

[186] Seaport and Cargo Security Hearing by Subcommittee on Crime, Terrorism and Homeland Security, 15 March 2005.

[187] Homeland Security Subcommittee Hearing on fiscal year 2006 appropriations, 15 March 2005.

dedicated lanes for clearance of trans-border shipments and reduced number of examinations. Participants of the FAST program are considered to be low risk and subject to faster inspection. CBP implements this along with C-TPAT, whose goal is to secure trade along nation's maritime borders. FAST is currently implemented at 11 of northern borders and 7 of southwestern borders.

Unlike C-TPAT, FAST program has not been supported with an initiative equivalent of CSI. Under the current regime, any threat has to be countered when it arrives at the land borders, and with possibly low level of valuable intelligence. Security measures are not extended beyond physical borders. We recognize that extension of land borders with an initiative may not be politically feasible due to sovereignty issues. The US government should work with both Canada and Mexico to improve intermodal transportation security in those countries to ensure safer conduct of land trade. Another approach to tackle the problem could be to introduce inspection facilities beyond borders before trucks reach the port of entry.

In particular, truck crossings from the southwestern border is vulnerable to weapon and explosive smuggling threat. Mexican trucks are not allowed beyond the 20 mile border zone in the United States. Therefore, Mexican long-haul carriers do not cross the border. Instead, they leave their load waiting for a Mexican drayage company truck to pick up the load on the Mexican side of the border. Then the drayage vehicle hauls the load to the American side of the border, where the load is picked up by an American truck to its final point of destination. This cumbersome process introduces two intermodal transfer points where the cargo container is exposed to tampering threat. An exception to this process is the crossing of maquiladora trucks.[188] Furthermore, trucks may wait a day or more for clearance across the border.[189] This causes extra delays and the cargo is laid possibly unattended at transfer points for long periods of time. Corruption and criminal activity, which is common in Mexico, has already affected containerized trade. Cargo theft is a huge problem in Mexico. According to the National Cargo Transport Chamber (Canacar) of Mexico, an average of 800 trucks is reported hijacked every year at a loss of $253 million.[190] Figures for truck robberies are more staggering: in 2001 figures were on the order of over 13,000 robberies per month.[191] Hijackers have the capability of emptying entire contents of a container within 30 minutes and leave.[192] As in maritime piracy case, many robbery and hijacking incidents go unreported. Maquiladora cargo is a preferred target for their economic value. All these figures suggest how vulnerable cargo is to tampering during transit phase in Mexico.

As in maritime cargo security case, empty containers or trailers pose another security threat. In 2002, 43% of the truck trailers that entered US from Mexico were empty.[193] However, as opposed to empty containers arriving at maritime ports, empty trailer trucks are subject to inspections. Truck safety related concerns and the history of drug smuggling across from the border triggered this inspection policy.[194] However, a thorough inspection of a 40-foot container may take as long as 3 hours.[195] This makes high inspection rates

[188] 'A maquiladora is a manufacturing plant, located in Mexico (usually near the US border) under foreign ownership, that typically has a sister plant on the US side of the border supplying parts to be assembled at the Mexican plant, that are then shipped back to the US.' Source: CRS Report to Congress, "North American Free Trade Agreement (NAFTA) Implementation: the Future of Commerical Trucking Across the Mexican Border", 22 September 2004.

[189] Efficient traditional shippers can expect paperwork delays of 4 to 5 hours. Source: See Footnote 185.

[190] John Suval, "Lawless Roads", Latin Trade, 1 March 2000.

[191] Ricardo Castillo Mireles, "Bienvenidos Amigos. Proceed with Caution", Transportation & Distribution, 1 March 2001.

[192] Scott Malone, "Cargo Theft Seen on the Rise", WWD, 17 June 2003.

[193] See Footnote 183.

[194] Drugs were found in empty trailer trucks on many occasions. See: "US Customs Service Inspectors Seize 2,362 Pounds of Marijuana at El Paso Port of Entry",www.cbp.gov , 8 March 2002. "234 Pounds of Cocaine Seized at Presidio Port", www.customs,gov, May 2002.

[195] "Transforming Border Management In the Post-September 11 World", Stephen E. Flynn. For empty containers,

impractical. Currently, all hazardous cargo trailers are inspected. Agricultural, food product, pharmaceutical and medical equipment shipments have priority in inspections. Empty trailers and other cargo are subject to secondary and thorough inspection if primary canine inspections, paperwork, driver behavior or the vehicle itself suggest that cargo may include illicit material.[196]

Background of truck drivers is critical to targeting high and low risk cargo. In particular, hazardous cargo drivers must go through an extensive background check. Under the FAST program, shippers who are already enrolled in C-TPAT should employ registered drivers who are in possession of a valid FAST-Commercial Driver Card. Drivers have to complete a single FAST Commercial Driver Application. Upon application, CBP reviews documents, and those who are admitted are further screened during an interview process, where fingerscans are taken and citizenship documents are reviewed. For other truck drivers, the inspection process may take longer time as the shipper or the importer is not participating in C-TPAT.

For Mexican drivers, a business visa, B-1 or B-2 is required to enter the United States. Mexican trucks make more than 4 million crossings a year into the United States. Under the NAFTA agreement, Mexican trucks would be allowed into the United States starting in 2002, however, due to environmental concerns and pressure from labor unions, full access was not granted. In June 2004, the US Supreme Court ruled that Mexican trucks can have access to US highways before environmental reviews are completed. [197] However, the Congress later voted on 20 November 2004 to restrict access due to safety reasons.[198] At the moment, the issue remains undecided, and recent NAFTA meetings did not produce any agreement towards this end. However, this regulation may introduce further risks to the homeland as criminal information of Mexican drivers will not be available to customs agencies. Mexican shipping companies may offer cheaper service that will further help US companies cut down their supply-chain costs. The US government should first cooperate with Mexican government to improve intermodal transportation security in Mexico before making a move in allowing Mexican drivers in the United States.

It is not clear whether the current border crossing practice will change in dramatic proportions if Mexican trucks are allowed into the United States. Border crossing is a cumbersome process due to traffic congestion. Therefore, long-haul companies would be less willing to commit their resources on border crossings. Furthermore, the degree of control exercised by Mexican customs brokers and close affiliation between them and drayage companies will slow down the transition to long-haul crossings. This increases the likelihood that cargo will be transferred from one truck to another at least twice in transit, continuing to introduce another point of vulnerability in the system.

Canadian truck drivers do not face similar access restrictions to the United States. Canada has initiated Partners in Protection (PIP) program which seeks cooperation of private industry for border security. PIP members are eligible to participate in FAST. Therefore, Canadian shipping companies have the opportunity to expedite their shipments like their American counterparts. Canadian companies participating in the program follow the same procedures in hiring trucks drivers. The risk is more an attribute for the drivers of the shippers not participating in either the PIP or FAST program.

Ports of entry are underequipped to detect nuclear and radiological bombs. CBP is installing radiological portal monitors nationwide, however, the process has been slow and most of the attention was given to maritime ports. The federal government will spend approximately $7 billion in coming years to install

inspections may take less time.

[196] See Footnote 185.

[197] “US High Court Clears Road Block to Mexican Trucks”, World Trade, August 2004.

[198] Angela Greiling Keane, “Congress Throws New Roadblocks Before Mexican Trucks”, Traffic World, 23 November 2004.

additional screening technology at maritime ports, land ports of entry and airports.[199]The goal is to screen %100 of all incoming goods, people and cargo for radiation. However, new equipment will likely suffer from high number of false positives as they don't discern nuclear weapons radiation from cat litter or ceramic tiles. Currently, %90 of the passenger vehicle traffic and %80 of the commercial truck traffic is inspected using radiation portal monitors on the northern border whereas half of the major ports of entry on the southwestern border are armed with radiation portal monitors.[200] Terrorists can exploit this vulnerability to introduce a dirty bomb in a container through a relatively less crowded port of entry. Another concern is lack of extra lanes for trucks going through radiological inspection. Congressman John Carter (R-TX) has drawn attention to trucks waiting in lines miles long at the ports of entry.[201] Hence, federal government should allocate funds to facilitate faster trade at these major ports of entry.

Another solution that was proposed by Stephen Flynn is to introduce "NAFTA inspection facility"s beyond the border.[202] A good implementation of this idea would be to introduce multiple facilities where trucks inspected earlier in transit could cross the next inspection facility without any interruption. A GPS device would be useful to minimize the risk of any route change between the inspection facility and the border crossing point. At the inspection facility, the truck would be issued a "proof of inspection" card, so that it can evade inspections at other facilities and border crossings. We believe that Mexican government can be motivated to cooperate if inspections are carried by Mexican customs officers as it would create further employment opportunities in Mexico. Like in CSI, American customs officers should be deployed to oversee inspections. Another advantage of this policy could be to reduce traffic congestions, helping the long-haul truck business to accept delivery of cargo to the final point of destination if free border crossing policy is enacted. However, this policy is likely to find a lot of opponents in Mexico raising sovereignty and funding issues.

As a part of NAFTA agreement, the US government should convince neighboring countries to improve their intermodal transportation security. A coordinated approach to increase security at cargo transfer points in North America will provide a very valuable shield against terrorism. Doing so, we have to recognize that cargo insecurity is not solely an issue for trucks operating in Mexico.[203] The US government should be proactive to propose such an initiative after a detailed evaluation of costs, and who should bear the cost.

2. Between Ports of Entry

Legal cargo does not move between ports of entry, however illegal aliens and their illegal contraband do, and have better chances to succeed in their mission to cross into the United States. Land borders can be classified under four categories. Federal lands are under the jurisdictions of Bureau of Land Management, Fish and Wildlife Service, and the National Park Service within the Department of the Interior, and the Forest Service within the Department of Agriculture. Indian tribal lands are under the jurisdiction of Bureau of Indian Affairs under Department of Interior, which assists management of tribal lands. State lands are managed by state agencies whose responsibilities range from regulating state parks and forests to other

[199] Eric Lipton, Mathew L. Wald, "US to Spend Billions More to Alter Security Systems", New York Times, 8 May 2005.

[200] During a hearing held by House Appropriations Subcommittee on Homeland Security on 15 March 2005, CBP Commissioner Robert Bonner quoted these statistics. He further added that a major border crossing point in the southwest will be covered by the end of FY 2006.

[201] Congressional hearing held by House Appropriations Subcommittee on Homeland Security on 15 March 2005.

[202] Written testimony before a hearing of the Committee on Foreign Relations United States Senate on "US-Mexico: Immigration Policy & The Bilateral Relationship": "Rethinking the Role of US-Mexico Border in the Port-9/11 World", Stephen Flynn, 23 March 2004.

[203] In fact, United States has serious transportation security problems that threaten cargo security. See "Cargo Theft Losses Total $12 Billion Annually", Modern Bulk Transporter, 01 December 2001.

natural energy resources. All these agencies employ their law enforcement officers to enforce federal laws and regulations in their respective lands. A fourth category is private lands along US borders. None of these agencies are directly responsible for interdicting illegal alien crossing through their lands. This mission is assigned to the US Border Patrol under DHS for the entire border.

a. Agencies, Programs and Resources in Border Line Defense

The Border Patrol is responsible from apprehension of illegal aliens and terrorists as well as interdiction of illegal drug, weapon and other contraband traffic. However, the Border Patrol has to work in coordination with law enforcement officers employed under different jurisdictions to fulfill its mission. Currently, the Border Patrol is employing 10,739 federal agents, almost 10,000 of which are responsible from the southwestern border. [204] As numbers suggest, most of the patrolling activity is at the southwestern border as Mexican border is notorious for being an illegal pathway for drug smugglers and illegal aliens. Patrolling operations are carried out on 20 sectors. President Bush proposed to add 210 more Border Patrol positions in fiscal year 2006 in an effort to beef up security along the northern border.[205] His proposal also includes $36.9 million appropriated for the Border Patrol activities.

The Border Patrol has a variety of technologies available for surveillance and enforcement. Infrared cameras and electronic ground sensors located at strategic locations are utilized to detect people and vehicle crossing borders illegally. Vehicles, boats and aircraft are used for patrolling missions. In some cases, horses are the main mode of patrolling in remote areas. The Border Patrol assists the Coast Guard in certain sections of maritime borders to interdict illegal aliens and smugglers. They also establish traffic checkpoints close to the border to detect those who have succeeded in an illegal entry mission and seeking to travel further inland on highways.

On the southwest border, the Border Patrol pursues a multi-layered border enforcement policy. The first layer is called line watch. Line watch agents are deployed to establish the first layer of defense against illegal alien traffic. The second layer, called line patrol, is deployed behind the line watch agents to provide support whenever needed. Both line agents keep high profile along land borders to deter illegal aliens. The third layer is located on highways or secondary roads to detect those who have avoided apprehension at the border.[206] There are 33 permanent interior checkpoints; all but one are along the southwest border. The goal is to direct illegal alien traffic to secondary roads, on which there is less traffic and the probability of apprehension is higher due to higher inspection rates. However, checkpoints on secondary roads are temporary and shifted based on incoming intelligence and on a random basis.

The US Border Patrol pursues “prevention through deterrence” strategy along the southwestern border. History of illegal contraband and human traffic, the welfare gap between two nations, and ongoing criminal activity beyond the border necessitate high profile presence along the border. However, with limited resources, this is a challenging task. Operation Safeguard which was launched in 1994, sought to increase Border Patrol presence along sections of the border that are close to population centers in Arizona. Operation Gatekeeper, which was initiated to stop high volume of traffic in '90's in San Diego sector was successful in reducing illegal border crossings. However, its macro scale effect was rather shifting of traffic to relatively unguarded sections of the border. Likewise, Operation Hold the Line, which seeks to deter illicit activity along the Texas-Mexico border, shifted the flow to other sectors. Regional successes in Operation

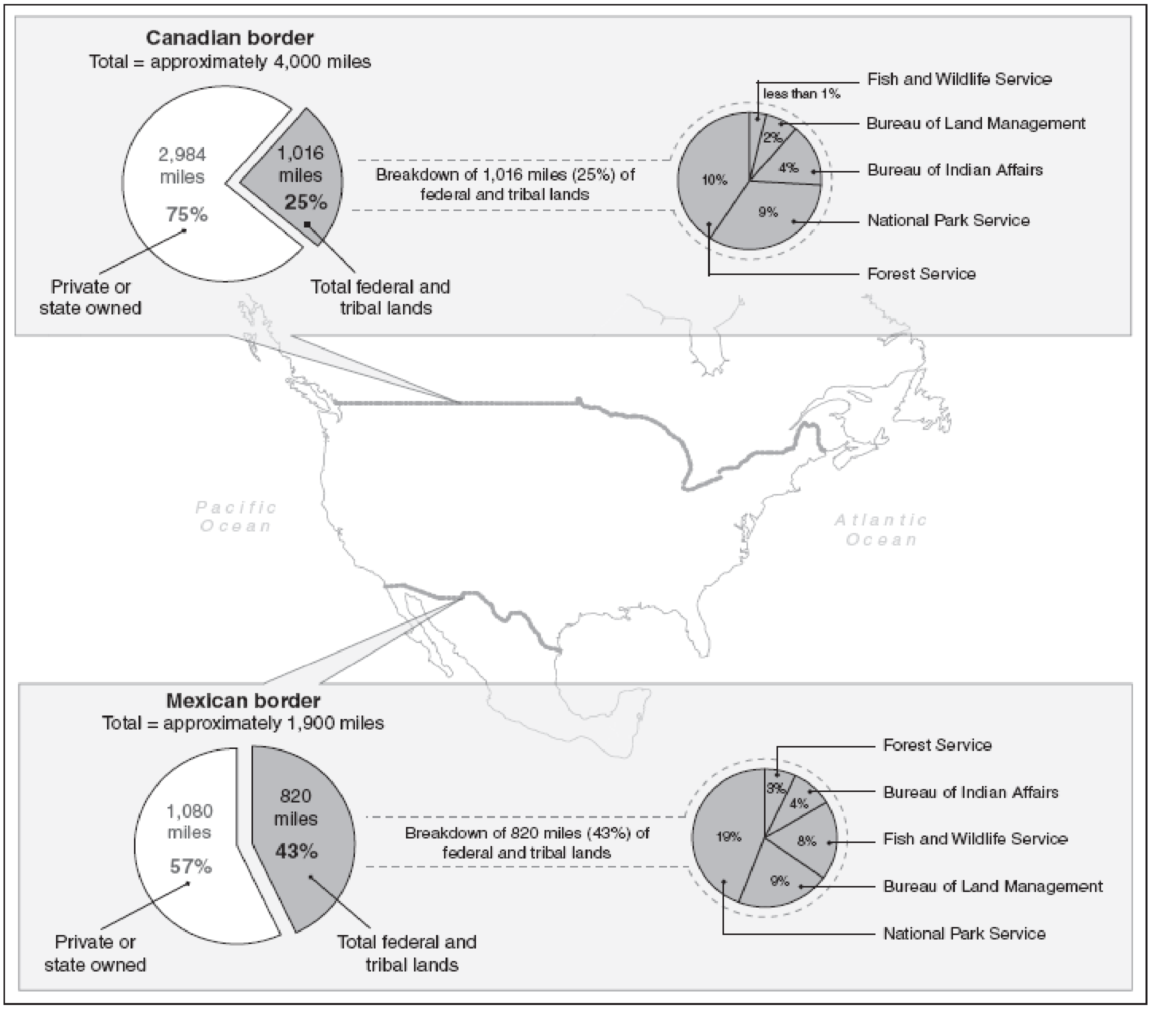
[204] Chris Strohm, “Activists to Flock to Border, Set up Citizen Patrols”, Government Executive, www.govexec.com, 28 March 2005.

[205] Congressional Hearing held by Senate Homeland Security and Governmental Affairs Committee, 9 March 2005.

[206] GAO Report, GAO-05-435, “Border Patrol: Available Data on Checkpoints Suggest Differences in Sector Performance”, 22 July 2005.

Gatekeeper and Hold the Line introduced extra challenges along the Arizona-Mexico border, and certain sections of the border started experiencing unusually high volume of activity. This urged the Border Patrol to launch Arizona Border Control (ABC) initiative in 2004. A different aspect of ABC is to bring federal, state and local authorities into border security efforts.

Figure 19 Percentage of Linear Miles of Federal and Trial Borderlands along Common Borders with Mexico and Canada[207]



US - Mexico partnership to reduce cross-border crimes have been generally to fight drug cartels, since drug smuggling is perceived as a common threat.[208] As far as the illegal alien traffic, we don't observe the same level of cooperation between both parties. Interior Repatriation Program is an exception. This program allows American officials to return Mexican apprehended crossing the border back to interior regions of the country. The goal of this initiative, which was launched in 2004, is to make a potential next crossing attempt

[207] Source: GAO Report, GAO-04-590, "Border Security: Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands", June 2004.

[208] More information on anti-drug traffic partnerships can be found in Anthony P. Placido's remarks before the House Committee on Government Reform Subcommittee on Criminal Justice, Drug Policy & Human Resources on "Threat Convergence along the Border: How Does Drug Trafficking Impact our Borders?", 14 June 2005.

inconvenient.[209]

Enormous length of the border, its challenging geography, large concentration of Canadian population north of the border and lack of large American population centers complicate efforts to guard the northern border.[210] Rather than deployment of huge number of agents along the northern border, Border Patrol have long sought and received cooperation from the Canadian side. The United States and Canada have established a relatively strong bilateral relationship in the last ten years to address common threats to national security. Both countries cooperate to address cross-border crimes through the United States – Canada Cross Border Crime Forum. Officials from Canada and the United States meet annually in this forum to discuss issues on various crime and terrorism. An important step to strengthen this mutually beneficial relationship came in 2001 when both parties signed the "The Smart Border Declaration". The declaration marked the beginning of active cooperation between both nations on specific border security. Canadian agencies support US efforts to defend the border through IBET initiative. This initiative seeks to increase intelligence sharing and coordination between American and Canadian agencies to detect and respond to criminal activity. Royal Canada Mounted Police (RCMP) maintains presence on the northern side of the border and provides support and personnel to IBET teams.

A recent effort to enhance land border security came with the announcement of Secure Border Initiative (SBI). SBI seeks to assume operational control of both the northern and southwestern borders in the next five years by hiring more USBP agents, upgrading technology and improving infrastructure. This initiative also sets a goal to strengthen interior law enforcement by providing funds to ICE to hire more criminal investigators. Increase in detention capacity and expediting removal of apprehended immigrants are among the improvements planned under SBI.[211]

b. Challenges in Border Patrol Operations

The Border Patrol is currently facing a unique set of challenges that render land borders vulnerable to terrorist penetration: inadequate staffing, insufficient technology, low morale and high attrition. In this section, we highlight some of the important aspects of these challenges. A good overview of these operational problems can be found in Garza (2005)[212].

More than four years after 9/11, the Border Patrol still does not maintain much presence along the northern border, mainly due to historically insignificant number of crossings. Statistics that seem insignificant in total number of crossings becomes significant when we consider the number of confirmed attempts to sneak through borders for terrorism purposes. Despite the triple size increase in the number of agents stationed across the border after 9/11, "the Border Patrol's ability to detect, respond to, and interdict illegal cross-border penetrations along the US-Canada border remains limited."[213] Similarly, the Border Patrol falls short of providing security along the southwestern border. Operational control of highly trafficked areas such as San Diego, El Paso and Mc Allen has been established, "however, many other areas along the southwest border are not yet under operational control, and the daily attempts to cross the border by thousands of illegal aliens from countries around the globe continue to present a threat to US national security."[214] President Bush's fiscal year 2006 budget proposal that provides funds for an additional 210 border patrol

[209] CRS Report for Congress, "Border Security: The Role of US Border Patrol", 10 May 2005.
[210] Ibid.
[211] More information is available on www.cbp.gov.
[212] Veronica Garza, "Vulnerabilities of the National Border Security Strategy on the US Border Patrol", CREATE DHS Scholar Report, 09 August 2005.
[213] National Border Patrol Strategy, CBP website, www.cbp.gov
[214] Ibid.

personnel falls well short of the mandate in Intelligence Reform and Terrorism Prevention Act of 2004 to increase in staff levels by 2,000 in the next 5 years.[215]

As the Border Patrol fails to match the targeted staffing levels, technology is an important element of border security that can fill the gaps. Geographical conditions at certain regions that render patrols impractical and sparse distribution of agents leave some sections unmonitored. A concerning fact is that the gaps are still not covered by proper technology. The Border Patrol's initial attempt to install an integrated system of cameras and sensors was subject to multiple failures,[216] unmanned aerial vehicles (UAVs) were not effectively used,[217] and equipment fell well short of covering the entire border. Technological limitations such as false alarms, or malfunctions under certain climate conditions introduce extra high-tech problems that the Border Patrol should confront.

Perhaps, one of the most important challenges reducing effectiveness of border patrols is low morale and high attrition rates. High rates of attrition was attributed in 2003 by CBP Commissioner Robert Bonner to the lack of job satisfaction, low pay compared to that other law enforcement officers performing similar tasks, lack of upward and lateral mobility, and poor working conditions.[218] This was corroborated by a personnel survey in 2004, in which most of the personnel expressed their concerns on lack of job satisfaction and poor management.[219] In the same survey, many interviewed drew attention to the lack of tools to effectively fight cross-border terrorism. High level attrition is a big challenge in maintaining adequate personnel along land borders. Another problem caused by high level of attrition is the lack of experienced personnel. Most of the inexperienced personnel are low pay agents. Low pay coupled with low expectations about future career leads to reduced performance and in some cases even corruption. Corruption incidents among the Border Patrol agents in the last five years reveal that drug smugglers have already exploited this vulnerability and crossed borders unimpeded.[220] Appropriate background checks are of paramount importance to reduce corruption. There is an urgency to address the factors that cause low motivation among the Border Patrol agents.

Non-technological resource limitation is another issue. For instance, law enforcement efforts on apprehended OTM aliens suffer from lack of detention bed space.[221] Most OTMs are released into the interior and are required to appear before the immigration judge. They cannot be sent back to Mexico because our southwestern neighbor does not accept non-Mexicans. Most of those released prefer not to show up for their hearings. The seriousness of the situation has been acknowledged by the President recently during his speech on border security and immigration reform.[222] He said,

> *We face a different set of challenges with non-Mexicans that we catch crossing the border illegally. When non-Mexican illegal immigrants are apprehended, they are initially detained. The problem is that our detention facilities don't have enough beds. And so, about four of every five non-Mexican illegal immigrants we catch are released in society and are asked to return for a court date. When the date arrives, about 75% of those released don't show up on the court. As a*

[215] Intelligence Reform and Terrorism Prevention Act of 2004, 17 December 2004.

[216] US House of Representatives, Minority Staff on the Committee on Homeland Security, "The US Border Patrol: Failure of the Administration to Deliver a Comprehensive Land Border Strategy Leaves Our Nation's Borders Vulnerable", May 2005.

[217] Ibid.

[218] See Footnote 205.

[219] Peter D. Hart Research, "Attitudes among Front-Line Border Protection Personnel", 20 August 2004.

[220] Veronica Garza, "Vulnerabilities of the National Border Security Strategy on the US Border Patrol", CREATE DHS Scholar Report, 09 August 2005.

[221] CRS Report for Congress, "Border Security: Apprehensions of 'Other Than Mexican' Aliens", 22 September 2005.

[222] He gave this speech at Davis-Monthan Air Force Base in Arizona. November 28, 2005.

> *result, last year, only 30,000 of the 160,000 non-Mexicans caught coming across our southwest border were sent home.*

Alternative policies should be developed to this issue if detention bed space will continue being short of meeting the demand. The government is working towards increasing the detention space. The Intelligence Reform and Terrorism Prevention Act of 2004 called for expansion of detention facilities by an average of 8,000 beds each year 2006 and 2010.[223] The Homeland Security Appropriations Act of 2006 includes funding towards achieving this objective. However, it is criticized to be short of the planned expansion; the number of beds will be increased by 4,000 in 2006.[224] Therefore, problems caused by the current catch and release policy are very likely to persist for several years to come.

c. Challenges on Federal, State, Private and Environmentally Sensitive Lands

Experts on terrorism know that terrorists and smugglers are adaptive to the environment and change their strategies quickly after new security measures are introduced. As the level of security is improved around historically well-known paths for illegal aliens, the influx shifts to relatively more remote, inhabitable and dangerous corners along land borders. The coordination between the Border Patrol and land management agencies is critical for success in these lands. According to GAO, the lack of coordination with the land management agencies caused problems in border apprehensions in remote areas. In particular, the Border Patrol did not consult to land management agencies, who may have detailed information about the terrain, in developing risk assessments. GAO report further points out problems of understaffing for the Border Patrol and land management agencies.

Some environmentally sensitive areas pose further challenges to implementing security measures to stop cross-border traffic. For instance, one of the security measures to build fences, steel walls or other forms of passenger and vehicle barrier along land borders has been sharply criticized by environmentalists on the grounds that the barriers will endanger the preservation of wildlife in the region. Environmentalists claim that these fences will limit the flexibility of wild animals to move across their habitat. Environmentalist groups are currently forming organizations such as The Northern Jaguar Project (NJP) and The Wildlands Project to raise awareness of these issues.

The Border Patrol has adopted the strategy of constructing barriers along land borders in early '90s as a part of “Prevention Through Deterrence” strategy. First border fencing was constructed in the San Diego sector, which used to experience high volume of traffic in early '90s.[225] However, this did not provide the expected level of deterrence. As a response, the USBP was authorized by the Congress to implement a three-tiered fence solution proposed by Sandia National Labs in 1993.[226] The apprehension statistics reveal a decreasing trend in traffic flow. However, there is no consensus whether this trend should be attributed to construction of fences. So far, 10.5 miles of this fence was constructed. Finishing the last 3.5 miles has been a challenge due to environmental concerns. In May of 2005, the Congress gave the DHS Secretary Michael Chertoff the authority to waive environmental laws when necessary. The Secretary used this authority for the first time when he made the decision to finish the last 3.5 miles of San Diego sector border fence.[227] Further barrier constructions are considered along the Arizona-Mexico border.

On the other hand, drug dealers have already resumed their illegal entries from waterways, forest and

[223] Vanessa Huang, “Watching the War on Terror”, ColorLines, Summer 2005.

[224] CRS Report for Congress, “Border Security: Apprehensions of 'Other Than Mexican' Aliens”, 22 September 2005.

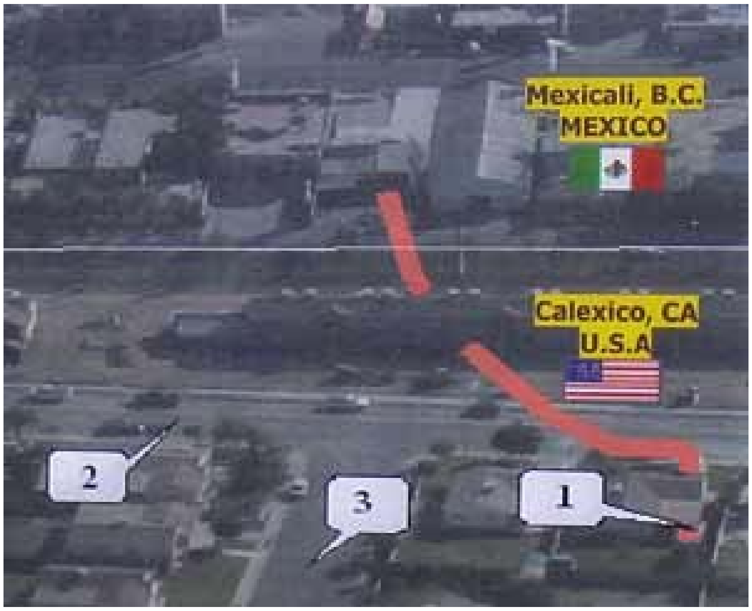
[225] CRS Report for Congress, “Border Security: Fences along the US International Border”, 9 May 2005.

[226] Ibid.

[227] Johanna Neuman, “US.Acts to Finish Divisive Border Fence”, Los Angeles Times, 15 September 2005.

wildlife refuges along the northern border.[228] According to GAO[229], marijuana seizures have increased from 2,600 pounds to 19,000 pounds between 2002 and 2003 in Ironwood Forest National Monument in Arizona. This was only a miniscule fraction of a total of 400,000 pounds of marijuana seized from 2000 to 2003 in national forests along the southwestern border. As of fiscal year 2003, the Fish and Wildlife Service's Cabeza Prieta National Wildlife Refuge was used as an entry point by an estimated 1000 undocumented aliens a week. All these figures suggest that trade-offs between security and environmental sensitivity will likely remain another point of debate in many years to come.

Figure 20 A Tunnel Route between Mexicali and Calexico, CA[230]



Another strategy that is recently employed by drug smugglers is crossing borders underground. Tunnels are dug in relatively urbanized areas where they can easily be concealed inside the apartment blocks. Before 9/11, border agents used to find only one such tunnel a year. However, this number has increased to more than 10 after 9/11 attacks.[231] Furthermore, both immigration and drug experts agree that there could be as much as 100 tunnels along the southwestern border. These tunnels are very convenient passageways to smuggle illegal weapons and explosives because the route into the United States is much shorter. It may be a relatively onerous task to smuggle a ballistic weapon across the desert.

d. The Minuteman Project

Public unrest about the failure to provide enough resources to the Border Patrol has grown significantly over the recent months. As a result, a group of volunteers has organized themselves under what they call Minuteman Project to patrol a 23 mile section of Arizona-Mexico border which is one of the most vulnerable points in the southwest, during the last month of April. Illegal immigration has shifted to this section of the border after the Border Patrol increased activities along the California-Mexico border. They sought to alert

[228] Sarah Kershaw, "Violent New Front in Drug War Opens on the Canadian Border", The New York Times, 5 March 2005.
[229] GAO Report, GAO-04-590, "Border Security: Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands", June 2004.
[230] Source: www.npr.com.
[231] "Tunnels Under the US-Mexico Border", NPR, 9 April 2004.

the Border Patrol about illegal crossings that have not been detected by the Border Patrol. The Border Patrol stated that illegal crossings have dropped 50% in Minuteman areas.[232] Chris Simcox, one of coordinators of this organization said that the project will be repeated in California, New Mexico and Texas until the Congress and the president take necessary actions to effectively seal borders.[233]

Mixed reactions surfaced about the project that lasted a month. Member of the House Judiciary Subcommittee on Immigration, Border Security and Claims, Congressman Lamar Smith (R-TX) said "If the federal government doesn't do its job, we shouldn't be surprised if citizens want to help protect their own property."[234] On the other hand, Congresswoman Sheila Jackson Lee described the project as "shame on the United States" as the "immigration is a federal issue", not a volunteer activity.[235] California Governor Arnold Schwarzenegger praised their efforts as "terrific", whereas President Bush called them "vigilantes".[236] Human rights activists raised concerns about mistreatment of illegal aliens by Minuteman members. Others have denounced the project on the grounds of unlawfulness and lack of training, while Congressman Tom Tancredo (R-CO) have expressed his sympathy by addressing the group as "heroes".[237]

Figure 21 One of the Many Trails Used by Smugglers on Arizona-Mexico Border[238]

CBP did not endorse the project and credited the decline of 50% in border traffic in the Minuteman terrain to increase in the number border agents patrolling the area and use of new aircraft. CBP recently increased the Border Patrol staff along the Arizona-Mexico border by 500[239] and Mexican government announced that they sent their own military to discourage people crossing the border as they were concerned about

[232] David Kelly, "Illegal Immigration Fears have Spread", Los Angeles Times, 25 April 2005.
[233] "Minuteman Set to Guard Mexican Border", NPR, 5 April 2005.
[234] Ed Gordon, "Undocumented Workers", NPR, 5 April 2005.
[235] Ibid.
[236] Ted Robbins, "Arizona's Minuteman Project Conclude this Weekend", NPR, 29 April 2005.
[237] "Volunteers to Patrol Arizona-Mexico border", www.cnn.com, 2 April 2005.
[238] Source: GAO.
[239] Chris Strohm, "DHS Beefs up Security along Arizona-Mexico Border", Government Executive, www.govexec.com, 30 March 2005.

possible confrontations. While, the contribution of the project to preventing illegal alien traffic is quite controversial, it is clear that the project has reached one of its goals to raise the issue of inadequate land border security nationwide.

e. Indian Tribal Lands

Indian tribal lands are among one of the most vulnerable points on American borders. While the Border Patrol has the responsibility for security of borders in their entirety, cooperation from tribal agencies is primarily required to prevent political repercussions that may ensue. More than 25 border tribes exist today, managing over 260 miles of land across the international borders.[240] However, they do not receive sufficient funding from DHS to improve homeland security. Therefore, there are minimal financial incentives for the Indian governments to enhance border security.

In the past, drug and human smugglers have heavily infiltrated into tribal lands. GAO estimates that an average of 1500 undocumented aliens crosses Tohono O'odham Indian Reservation each day.[241] This figure may have recently dropped as the local police have cooperated with the Border Patrol to conduct operations against illegal immigrants. Akwesasne Reservation on the northern border is a "major smuggling hub for goods illegally transported in and out of Canada from US or vice versa including narcotics, firearms, alcohol, tobacco and illegal aliens".[242] Even some tribal members in this reservation were found connected to some of the human smugglers.[243] A more troubling record is the charge in 1999 on Mohawk tribe members in New York for allegedly helping Al-Qaeda operatives cross the border.[244]

Many Indian governments have built casinos that attract many tourists to their reservations. In particular, reservations along the Canadian border are highly vulnerable for illegal crossing as the Canadians have a free access to casinos on the border with minimal identity check. Terrorists who may already be stationed in Canada can exploit this vulnerability. The Border Patrol operations are highly controversial in those areas as some tribal members view those as a violation of their "sovereignty" across their reservations. Some tribal communities go even further to demand treatment of s separate sovereign nation from the US government. The degree of sovereignty of local governors on Indian tribal lands may be a block to enhancing border security. The US government should focus more on communicating the threats to Indian reservations and clarify her position against global terrorism. Cooperation should be sought to ensure the help of local tribesmen who may have specific intelligence about their reservations. The government should move forward to distribute federal money to Indian communities for counter terrorism measures.

Homeland security should not be compromised to political rifts between local and federal governments. If the tribal governors do not move forward to cooperate with the federal agencies, then a security zone along the perimeters of tribal lands may be a necessity to confine the potential terrorists to border reservations and deter them from penetrating further into the homeland.

The Border Patrol needs more staff and more equipment to properly fulfill its mission. An estimated influx of 3-4 million illegal aliens makes this country extremely vulnerable to terror. No one knows what the next attack would be like. However, if we discover that a catastrophic attack is launched by terrorists illegally crossing borders between ports of entry, the government's next step could be as radical as laying mines or

[240] "President Bush's Budget Undermines Basic Needs of Tribes", Sho-Ban News, 10 February 2005.
[241] GAO Report, GAO-04-590, "Border Security: Agencies Need to Better Coordinate their Strategies and Operations on Federal Lands", June 2004.
[242] Jan Golab, "The Festering Problem of Indian 'Sovereignty'", The American Enterprise, September 2004.
[243] Katherine McIntire Peters, "Difficult Terrain", Government Executive, 1 April 2004.
[244] Jan Golab, "The Festering Problem of Indian 'Sovereignty'", The American Enterprise, September 2004.

increase military presence to dramatically high levels in an attempt to completely seal borders. While this solution is far from our imagination at this point, we should realize the extent of threat to the civil liberties and openness of this society to foreign individuals who contribute to the economy and scientific research. There is an urgency to act before something catastrophic happens at or originating from the borders.

V. AVIATION SECURITY

Gaps in aviation security were highlighted by the 9/11 attacks on the Twin Towers and the Pentagon. 9/11 changed the way Americans look at the security measures on airlines, as one of the basic assumptions was completely demolished. In the new era, a terrorist on an airplane may engage in an activity that may endanger his life if the attack is expected to do much greater harm. In this regard, 9/11 signaled a return back in time to *kamikaze* years, when Japanese pilots launched suicide attacks on American targets. As the persistence of terrorists to harm American interests and lives have been revealed, the federal government moved forward to impose more strict security measures that would minimize the chances of use of airplanes as a weapon on a homeland target or as a path to cross American borders to launch attacks inland. Congress passed the Aviation and Transportation Security Act (ATSA) in November 2001, which created Transportation Security Administration (TSA) under Department of Transportation (DOT). TSA was later moved under DHS in 2002 as a result of the Homeland Security Act.

Table 9 Major Attacks on American Airliners in the Last 30 Years[245]

Year	Event
1975	A bomb exploded in New York City's La Guardia Airport, killing eleven and injuring seventy five, leaving an economic damage of $750,000. Palestinian Liberation Organization assumed responsibility.
1979	A mail bomb exploded in the cargo section of an American Airlines jetliner with 88 passengers flying from Chicago to Washington. The plane made a successful emergency landing at Dulles International Airport. The attack was later claimed by an Iranian student group protesting deportation of Iranian students from the United States. No one was injured.
1982	As a result of the explosion in Pan American World Airways Boeing 747 jetliner, one passenger was killed, and 14 were injured. The plan successfully landed in Honolulu, Hawaii. PLO was believed to be responsible.
1985	TWA Airliner was hijacked to Beirut by Hezbollah and held for 17 days. One US Navy diver was executed.
1986	A Pan Am Boeing 747 was hijacked by Abu Nidal Organization. 19 passengers were killed, 127 were wounded.
1986	A bomb exploded on a TWA jetliner over Greece. The emergency landing was successful. Abu Nidal claimed the responsibility. There were 4 casualties and 9 injuries.
1988	Pan Am Flight 103, flying from London to New York, exploded in the air, and crashed in Scotland. 259 on board, 11 on the ground were killed, 12 were seriously injured. Palestinian groups, Libya and Iranian revolution sympathizers are believed to be behind the attack.
1996	TWA Flight 800 exploded over Long Island after taking off for Paris. 230 passengers died in the attack. The reason of explosion is still controversial.
2001	Al-Qaeda hijacked two American Airlines and two United Airlines jetliners to attack World Trade Center and Pentagon. In this catastrophic incident, around 2,800 were killed, and hundreds were injured.
2002	An Egyptian-born man opened fire at the Israeli Airlines ticket counter at the Los Angeles Airport, killing two and wounding three.

Terrorism in the air has always been warranted more media coverage than other means to launch terrorist

[245] Source: Terrorism Knowledge Database, www.tkb.org

attacks. This helped terrorists put more pressure on the governments to concede their political and financial

Table 10 History of Airline Hijacking[246]

Date	Location	Carrier	Fatalities	Group Responsible
7/22/1968	Rome	El Al Israel Airlines	0	Popular Front for the Liberation of Palestine
6/17/1969	Oakland	TWA	0	Black Panthers
8/29/1969	Paris	TWA	0	Popular Front for the Liberation of Palestine
7/22/1970	Beirut	Olympic Airways	0	Palestinian Popular Struggle Front
9/6/1970	Amsterdam	Pan Am Airlines, Swissair, TWA	0	Popular Front for the Liberation of Palestine
6/2/1972	Seattle	Western Airlines	0	Black Panthers
6/31/1972	Florida	Delta Airlines	0	Black Panthers
11/24/1972	Frankfurt	Air Canada	0	An armed gunman
7/20/1973	Amsterdam	Japan Airlines	0	Organization of Sons of Occupied Territories
11/21/1974	Dubai	British Airways	1	Palestinian militants
4/7/1976	Philipinnes	Not specified	0	Moro National Liberation Front
9/10/1976	New York	TWA	1	Croation Freedom Fighters
7/8/1977	Beirut	Kuwait Airways	0	Palestinian militants
10/13/1977	Spain	Lufthansa	1	Popular Front for the Liberation of Palestine
4/4/1979	Sydney	Pan Am Airlines	0	An armed man
6/20/1979	New York	American Airlines	0	A Serbian nationalist
1/18/1980	Beirut	Middle East Arlines	0	Amal
1/28/1980	Baghdad	Middle East Arlines	0	Amal
10/13/1980	Istanbul	Turkish Airlines	0	Amal
12/15/1980	Bogota	Avianca Airlines	0	M-19
3/28/1981	Indonesia	Garauda Indonesian Airways	0	Komando Jihad
5/24/1981	Istanbul	Turkish Airlines	0	DHKP-C
9/29/1981	New Delhi	Indian Airlines	0	Sikh militants
12/7/1981	Zurich	Libyan Airlines	0	Amal
12/7/1981	Venezuela	Three Venezuelan Airliners	0	Puerto Rican independence fighters
2/25/1982	Beirut	Kuwait Airlines	0	Shite militants
6/23/1983	Athens	Libyan Airlines	0	Amal
7/31/1984	Frankfurt	Air France	0	Guardsmen of Islam
8/24/1984	New Delhi	Indian Airlines	0	Sikh militants
12/4/1984	Tehran	Kuwait Airlines	2	Hezbollah
6/7/1985	Athens	TWA	1	Hezbollah
6/11/1985	Beirut	Royal Jordanian Airlines	0	Amal

[246] Source: Terrorism Knowledge Database, www.tkb.org

Table 10 History of Airline Hijacking continued

Date	Location	Carrier	Fatalities	Group Responsible
6/12/1985	Larnaca	Lebanese Airlines	0	Palestinian militants
9/5/1986	Karachi	Pan Am Airlines	19	Abu Nidal
12/25/1986	Baghdad	Iraqi Airways	67	Hezbollah
6/27/1987	Brazzaville	Air Afrique	1	Hezbollah
4/5/1988	Bangkok	Kuwait Airlines	2	Hezbollah
11/9/1991	Russia	A Russian Airline	0	Chechen Guerillas
3/27/1996	Luxor	EgyptAir	0	Bani Hilal Tribe
11/23/1996	Ethiopia	Ethiopian Airlines	127	Ethiopian militants
8/18/2000	Azerbaijan	Azerbaijani Airlines	0	Opposition Group
8/24/2004	Rostov-on Don	Sibir Airlines	46	Riyad us-Saliheyn Martyrs' Brigade

demands. This combined with lax security measures paved the way for a rich history of airline terrorism. Most airline attacks in the past have been in the form of hijacking and detonating explosives. Tables 9 and 10 give a summary of major attacks on US airliners and successful hijacking incidents.

Airline attacks on aviation have increased significantly in the late ‘60s and kept its high frequency until early ‘90s. In the early days of airline terrorism, security measures were minimal providing variety of options for the armed guerilla to launch attacks. For instance, terrorists could conceal weapons and explosives in checked baggage, or find inside collaborators to launch deadly attacks. Before September 11, screening of baggage and passengers were not properly addressed.

Prior to 9/11, Federal Aviation Administration was responsible for aviation security in the United States. With ATSA, the responsibility was transferred to TSA. With the renewed urgency in aviation security, Congress shifted its focus on the implementation of a number of measures by creating TSA. Although TSA was primarily involved in ensuring security in all modes of transportation, aviation security was the priority as TSA were to meet a tight schedule to implement security measures.

Aviation security can be analyzed under several categories. However, all aspects of aviation security are not necessarily interwoven with border security. For the purposes of this report, we will elaborate more on screening of passenger baggage and cargo, passenger identity checks, and some issues related with workers at the airports such as background checks and their access to secure areas. On the other hand, there is no discussion provided on airport perimeter security. While terrorism risks posed by gaps in airport perimeter security may be greater than those posed by the issues discussed in this report, they do not necessarily originate beyond US borders.

A. Vulnerabilities in International Air Transportation

Since the September 9/11 attacks, TSA has made considerable progress to improve aviation security and helped the bleeding airline industry to continue conducting business. The pace in hiring of new employees to perform screening duties, and deploying the necessary technology to increase baggage transparency was remarkable. For instance, in its first year alone, TSA hired 65,000 passenger and baggage screeners and deployed explosive detection equipment to ensure 90% passenger baggage screening[247]. However,

[247] GAO Testimony, GAO-03-1150T,”Aviation Security: Progress Since September 11, 2001 and the Challenges Ahead”, 9 September 2003.

vulnerabilities still remain, particularly in screening of cargo and passenger identity checks.

1. Passenger and Baggage Screening

Among the worst airline disasters in history are those attributed to explosives on passenger baggage or air cargo. Prior to 9/11, screening of passenger baggage and air cargo was the responsibility of commercial airlines. At the time, FAA characterized the screeners' performance in detecting threat objects on passengers and in their carry-on luggage less than satisfactory.[248] FAA testing on assessing the performance of screeners showed that screeners' ability to detect objects declined significantly as test cases became more realistic representations of what terrorists would have done in a similar situation. GAO attributed these errors to the lack of experience and training of screeners due to high turnover. Most skilled screeners were paid low and thus quit their jobs, leaving all the screening jobs to those with minimal experience. Another reason according to GAO study was the monotonous nature of screening work leading to low morale and lack of motivation.

Table 11 shows some of the commercial airline disasters due to aircraft explosions. There has been near other near misses in recent aviation history. One striking example is the plot to blow up 12 US aircrafts over the Pacific in 1995, which was discovered by Philippine authorities.[249] Although aviation history had sufficient number of wake up calls for terrorists' intentions to harm the industry and people by locating explosives on the airplanes, none of these vulnerabilities were properly addressed prior to 9/11.

Table 11 Commercial Airline Bombing Disasters

Date	Location	Carrier	Fatalities	Group Responsible
2/21/1970	Zurich	Swissair	47	Popular Front for the Liberation of Palestine
10/6/1976	Barbados	Cuban Airlines	73	Anti-Castro Cubans
6/23/1985	Montreal	Air India	329	Sikh militants
4/2/1986	Bangkok	TWA	4	Abu Nidal
11/29/1987	Abu Dhabi	Korean Airlines	115	North Korean government suspected.
12/21/1988	Scotland	Pan Am Airlines	270	An assembled terrorist group allegedly supported by Libya and Iran

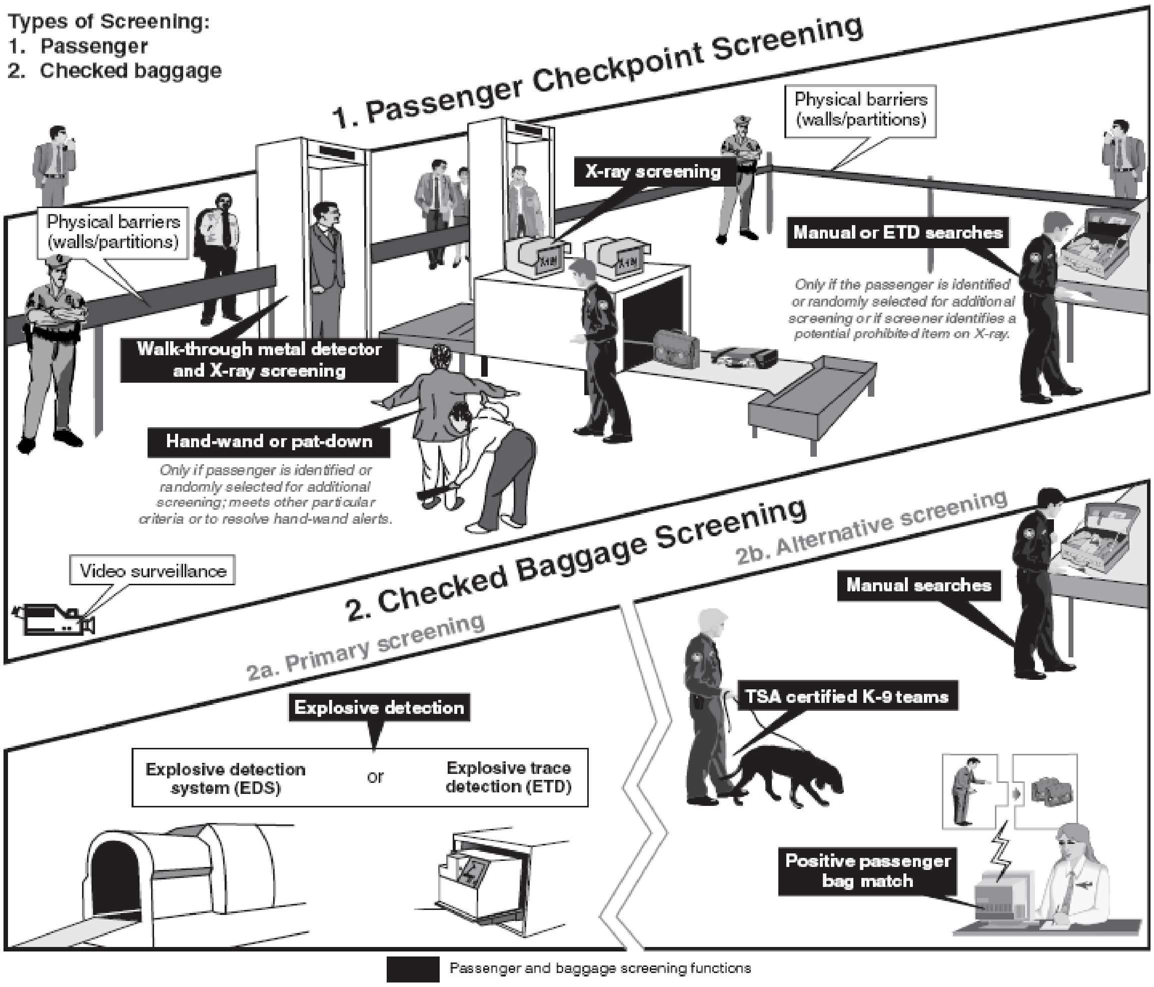
As the commercial airline practice of managing screening process proved ineffective, the Congress assigned responsibility to TSA. In its first year, TSA hired, trained and deployed 40,000 workers to screen the passengers and 20,000 to screen the checked baggage. By the end of 2002, the 90% of the checked baggage was screened in all the airports. The ultimate goal for checked baggage is attaining %100 baggage screening, which has not been fully satisfied to this date. GAO reported that TSA deployed the necessary technology for %100 screening, however due to skilled screener and equipment shortages fell short of attaining the goal at over 440 commercial airports nationwide.[250]

There have been imbalances in employing this labor force in the areas of need. As a result, GAO believes that some airports had too many screeners whereas some had less than required. The main reason for this imbalance is the high attrition rates. The average attrition rate for screeners has been 14%. In some airports, the attrition rate has been as high as 36%, which is one of the main reasons for the lack of trained

[248] GAO Testimony, GAO-01-1166T, "Aviation Security: Terrorist Acts Illustrate Severe Weaknesses in Aviation Security", 20 September 2001.
[249] Nicholas D. Kristof, "Why didn't we Stop 9/11?", The New York Times, 17 April 2004.
[250] GAO Testimony, GAO-04-440T, "Aviation Security: Challenges Exist in Stabilizing and Enhancing Passenger and Baggage Screening Operations", 12 February 2004.

and experienced screeners at some airports. GAO study showed that 11 of 15 high security risk (category X) airports suffer from staff shortages. Hiring new screeners to fill the vacant positions has not been easy either. Screening jobs are not attractive even for part time employees; offering a monotonous work environment at relatively undesirable work hours. Many candidates recognize that they will have to serve overtime hours as long as staff shortages continue. In order to address the problem of screener shortages, TSA established a National Screening Force in October 2003 to support the airports' emergency staffing needs. At least 50% of this extra work force has been employed at high risk airports.

Figure 22 Passenger and Checked Baggage Screening[251]


Types of Screening:
1. Passenger
2. Checked baggage
1. Passenger Checkpoint Screening
Physical barriers (walls/partitions)
X-ray screening
Manual or ETD searches
Only if the passenger is identified or randomly selected for additional screening or if screener identifies a potential prohibited item on X-ray.
Physical barriers (walls/partitions)
Walk-through metal detector and X-ray screening
Hand-wand or pat-down
Only if passenger is identified or randomly selected for additional screening; meets other particular criteria or to resolve hand-wand alerts.
Video surveillance
2. Checked Baggage Screening
2b. Alternative screening
Manual searches
2a. Primary screening
Explosive detection
Explosive detection system (EDS)
or
Explosive trace detection (ETD)
TSA certified K-9 teams
Positive passenger bag match
■ Passenger and baggage screening functions

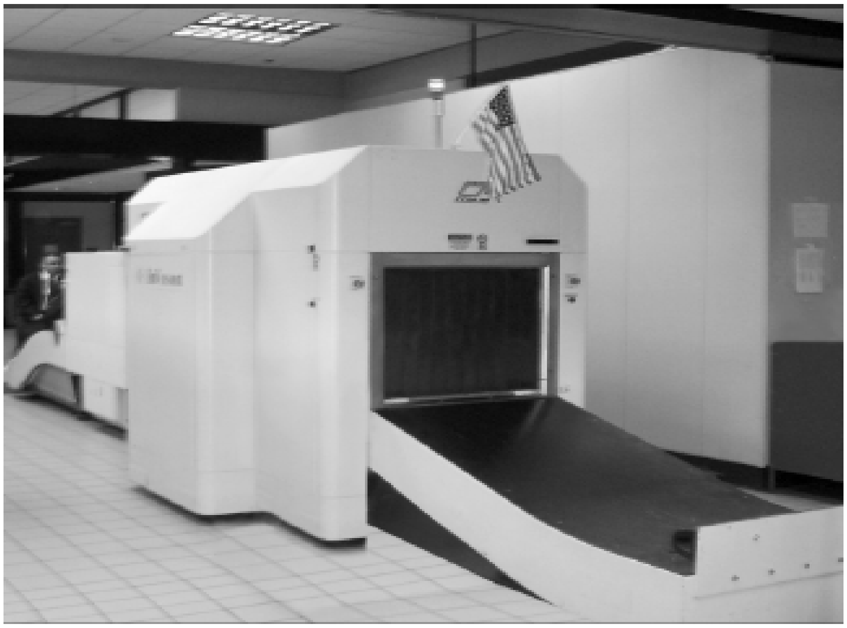
According to GAO, problems exist in passenger and baggage screener training. As most of the screeners lack experience, screener training is one of the key factors that will ensure a satisfactory performance in detection. Training seeks to improve recognition of X-ray images of threat objects and detection of explosives on passenger baggage. With the increase in hours that screeners need to allocate on their job, it became harder to find the time slot for training and difficulties in accessing online courses reduced the effectiveness of training programs.

TSA is conducting multiple tests to assess the performance of screeners. Covert tests are conducted

[251] Source: GAO.

unannounced to assess the screener performance. TSA agents make an attempt to pass threat objects through checkpoints. Covert tests revealed weaknesses in identification of threat objects on passengers and baggage. Threat Image Projection (TIP) is a test designed to train screeners by projecting threat images onto bags as they are screened during actual operations. The test is available for passenger screening, but not available for screening checked baggage. Recertification testing is conducted to fulfill the ATSA requirement that each screener's qualifications are reviewed annually to check if they meet the standards. Each screener has two chances to pass the test, and those who fail in the second attempt are not employed at screening points. These tests are mostly available for passenger screening and similar training and testing modules for checked baggage is still in development phase.[252] President's fiscal year 2006 budget requests $91 million to implement training programs.[253] Another $ 174 million is requested for installation of high speed internet connectivity.

Figure 23 EDS Machine[254]



Explosives Trace Detection (ETD) and Explosives Detection System (EDS) technologies are used to inspect checked baggage. EDS machines use computer aided tomography X-rays to recognize explosives whereas ETD machines do a chemical analysis to detect chemical residues and vapor from explosives. Between 2002 and 2004, TSA spent $2.5 Billion of its $2.7 Billion total budget on procurement and installation of these machines. TSA has procured 1200 EDS machines and 6000 ETD machines and installed them at over 440 commercial airports.[255] EDS machines cost approximately $1 Million each, whereas a single ETD machine can be purchased for $40,000. On the other hand, an ETD machine is more labor-intensive and can process only 40 bags per hour whereas and in-line EDS machine can process 425 bags per hour. ETD machines account for majority of bag inspections at smaller airports. For higher

[252] GAO Report, GAO-05-457, "Aviation Security: Screener Training and Performance Measurement Strengthened but More Work Remains", 2 May 2005.

[253] GAO Testimony, GAO-05-357T, "Transportation Security: Systematic Planning Needed to Optimize Resources", 15 February 2005.

[254] Source: GAO.

[255] GAO Report, GAO-05-365, "Aviation Security: Systematic Planning Needed to Optimize the Deployment of Checked Baggage Screening Systems.", 15 March 2005.

category airports, EDS machines are used extensively for checked baggage screening. For instance, %70 of checked baggage is screened with EDS machines in a category X airport, leaving only %18 to ETD machines and %12 to other approved methods such as canine inspections.[256]

During the installation phase of EDS and ETD machines, airport facilities had to be modified and interim solutions were developed to meet the Congressional deadline. At the moment, these machines are not fully integrated with the airport's baggage handling system. According to GAO, this caused operational inefficiencies, such as allocation of more staff than required and a slower pace in screening. Furthermore, it leads to formation of long queues, which is another security problem by itself. TSA seeks to abandon interim solutions and finish permanent in-line baggage screening system installations by March 2007. When the in-line systems are installed, the screening of checked baggage will be faster and staff requirements will decrease. The cost of installing in-line baggage systems is estimated to be between $4 billion and $5 billion nationally, excluding the cost of machines.[257]

Figure 24 ETD Machine in Use[258]

Screening Partnership Program (opt-out program) has been developed by TSA to allow airports to hire private screeners instead of those employed by TSA. After a two year pilot program TSA began accepting applications for the program in November 2004. Private companies owned and controlled by US citizens can participate in the program. All private screeners should go through background criminal checks and should have at least a high school diploma. According to GAO, potential benefits of this program have not yet been realized. As far as performance, private and federal screeners have revealed minimal difference,[259] and there are issues waiting to be resolved on the flexibility of private companies in the hiring process and the degree of liability in the case of a failure that results in a terrorist attack.[260] Private screening program has the potential to eliminate some of the operational inefficiencies like unbalanced allocation of screeners across airports and high attrition rates. This could potentially increase the percentage of highly experienced screeners at the airports. As screening performance is still less than

[256] GAO Testimony, GAO-05-896T, "Aviation Security: Better Planning Needed to Optimize Deployment of Checked Baggage Screening Systems", 13 July 2005.

[257] Congressional Testimony on aviation security by David Z. Plavin on 12 February 2004.

[258] Source: www.boeing.com.

[259] GAO Testimony, GAO-04-505T, "Aviation Security: Private Screening Contractors Have Little Flexibility to Implement Innovative Approaches", 22 April 2004.

[260] GAO Report, GAO-05-126, "Aviation Security: Preliminary Observations on TSA's Progress to Allow Airports to Use Private Passenger and Baggage Screening Services", November 2004.

satisfactory according to tests conducted so far, TSA should move forward to address training and motivational requirements of screeners.

Despite all the efforts and funding support to improve passenger and baggage screening, 9/11 Commission recently found the progress made so far less than satisfactory. The Report Card released in December 2005 assigns a letter grade C to passenger and carry-on baggage screening and D to checked bag and cargo screening. The main criticism is on the failure to install in-line systems which results in reduced efficiency and throughput. The next challenge in improving aviation security will be to complete appropriate layout changes at the airports to accommodate in-line baggage screening systems and ensuring a steady flow of funds to pay high costs of this ambitious undertaking.

International aviation industry has long sought to improve security after Pan Am Flight bombing in 1988. United Kingdom has taken the lead in European Union to set 100% screening goal for carry-on and checked baggage in 1996. International bodies such as International Air Transport Association (IATA) and European Civil Aviation Conference (ECAC) have urged its member states to accomplish 100% screening goal using X-ray detection technology. In December 2002, European Union Transport Council has adopted the recommendation made by ECAC in its common rules in the field of aviation security. According to a recent report by the Commission of the European Communities, significant but uneven progress has been made so far to this end.[261] European approach in baggage screening is risk based, in which only suspicious baggage are screened by EDS machines while most baggage are screened by second-tier automated X-ray machines.[262] Canada is also dedicated to 100% screening of checked and carry-on baggage. In December 2001, Canadian government initiated a five year plan to spend $1 Billion a year to acquire and install EDS machines to cover 99% of air traffic.

Some experts believe that passenger and baggage screener performance in some European countries has been better than in United States. For instance, according to an FAA study conducted in one undisclosed European country revealed that screeners are able to identify twice as many threat objects than in United States.[263] This was attributed to better pay, benefits and more stringent screening operations. Some screeners are trained to conduct interviews with passengers before international flights. Furthermore, ECAC provides support to member states to improve screener training.[264] In short, aviation security has been improved incrementally in most other states as terrorism has hit commercial air traffic rather uniformly across the globe. To the best of our information, an overall comparative assessment of aviation security status between United States and other nations is not yet available. However, most international bodies are taking terrorism threat seriously and work to reduce vulnerabilities in commercial aviation.

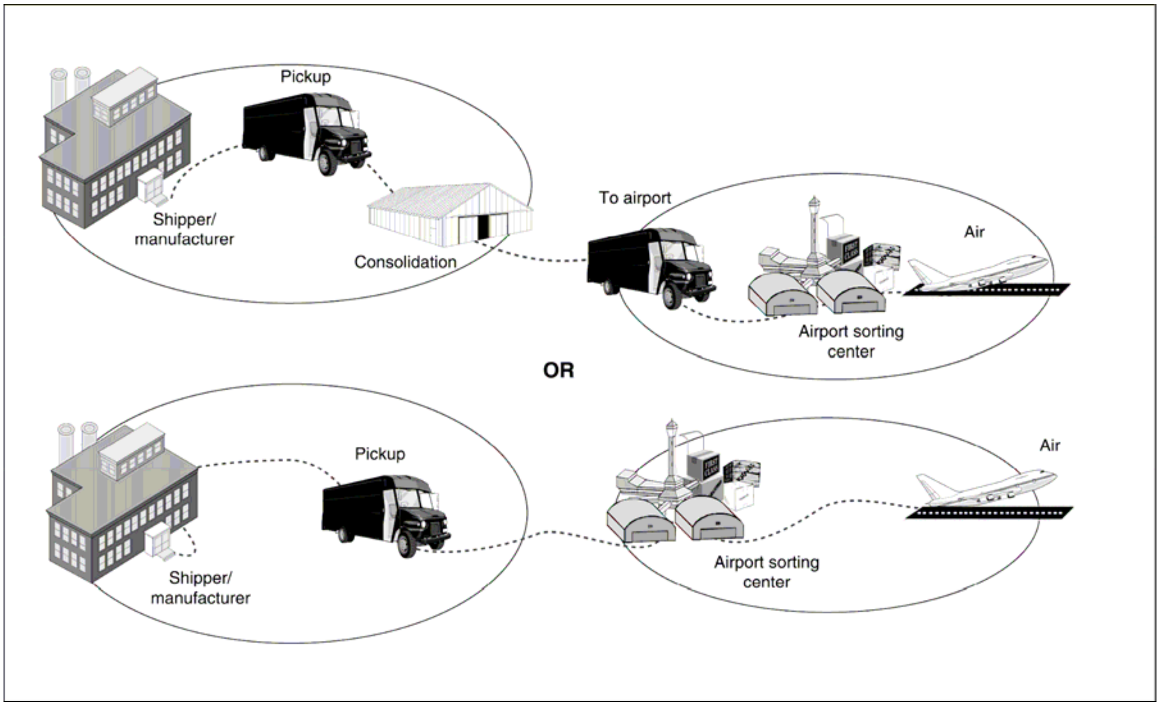
2. Air Cargo

Screening of air cargo is one of the most vulnerable points of aviation security. Transportation of air cargo, as Figure 25 illustrates include three parties, manufacturer or shipper, freight forwarder and an air carrier. Freight forwarder transports the shipment from a manufacturer or shipper to an air carrier. They may serve multiple shippers. In order to minimize transportation costs, freight forwarder may consolidate multiple shipments before delivering to an air carrier. Shippers that require more urgent processing for their cargo may skip freight forwarders, and directly deliver the cargo to air carriers. More than 20% of all air cargo is

[261] Commission of the European Communities, “First Report on the Implementation of Regulation 2320/2002 on Civil Aviation Security”, 3 October 2005.
[262] Robert W. Pole and George Passantino, “A Risk Based Airport Security Policy”, May 2003.
[263] GAO Testimony, GAO-01-1165T, “Aviation Security: Weaknesses in Airport Security and Options for Assigning Screening Responsibilities”, 21 September 2001.
[264] For example, ECAC TIP library has been made available to member states in 2004.

transported on passenger aircrafts, whereas the rest is carried on cargo planes. In addition to general cargo, air carriers also transport mail.

Figure 25 Flow of Air Cargo[265]



GAO's December 2002[266] report outlined vulnerabilities in air cargo transportation system. Most of the vulnerabilities have been identified by the Gore Commission's study in 1996. Vulnerabilities in air cargo and in cargo shipment by other modes of transportation are quite similar. Tampering with cargo while in transit on the ground, or at consolidation centers, security violations during the loading phase, hiring workers with criminal backgrounds at loading facilities and cargo theft at consolidation centers are among the common problems that should be addressed in ensuring secure transportation of cargo in all modes. GAO reported that TSA has already identified security violations by freight forwarders. According to FBI, most of the air cargo thefts in the United States occur at transfer facilities, cargo terminals and consolidation centers.

TSA announced the Air Cargo Strategic Plan in November 2003. This is a threat based risk management approach that seeks to identify priorities in improving air cargo security. TSA has already finished threat assessments on air cargo security. As in the sea cargo and the land cargo case, development of methodologies to perform targeted cargo inspections, deploying technology that will enable faster and efficient screening of cargo, and development of technology that will prevent possible tampering with air cargo are among the priorities. As in Automated Targeting System for the sea cargo, this strategic plan initiated a program to target and screen high risk cargo. The Freight Assessment System will use information on known shippers and air carriers to determine high risk cargo. The Known Shipper Program seeks to identify the companies with "trusted" shipments. Data on known shippers will be fed in the Freight Assessment System to assign a risk level for the shipments. The Freight Assessment System will check

[265] Source: GAO.
[266] GAO Report, GAO-03-344, "Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System", 20 December 2002.

terrorist watch lists and other intelligence information and reflect this information to evaluation of the risk level that cargo poses. The president's fiscal year 2006 budget proposes allocation of $40 million in improving air cargo security. This financial resource will be used to bolster continuing programs and identify requirements for Indirect Air Carriers such as freight forwarders. One objective is to augment the Known Shipper Program to prohibit air carriers from accepting cargo that does not originate from shippers following the Known Shipper Program's requirements.

One key requirement of the system is establishing a consolidated database of known shippers that will store the identity of those known to carriers. TSA has already constructed this database, but less than one-third of the estimated 1.5 million known shippers have registered their information so far.[267] Testing of the Freight Assessment System that will use data on shippers to select low and high risk shippers is expected to be completed early 2006. However, with information on less than one-third of known shippers, quality of targeting results will be questionable. Currently, TSA conducts random inspections on air cargo shipments. These inspections include physical searches and use of non-intrusive technology. Some types of cargo are exempt from inspections as TSA believes they pose minimal security risk.[268] These exemptions are effective on both passenger and all-cargo aircraft. As opposed to baggage inspections on passenger aircraft, all the security measures are implemented by air carriers under the operational direction of TSA. Each air carrier maintains a separate database of known shippers that they have built a trustworthy business relationship over time. Air carriers also have the right to deny shipments from "unknown" shippers. This seems to be only layer of security for air cargo at this point, apart from the random inspections, because most air carriers limit their business to those in their known shipper list.[269] However, experts raised concerns about the insufficiency of investigations required to grant known shipper status.[270]

Experts estimate that 10% of air cargo is physically inspected.[271] TSA maintains the belief that the Known Shipper Program's requirements on air carriers and freight forwarders prescreen the companies involved with air cargo trade and mitigate risk effectively. However, pilots involved in this business for many years believe that "the Known Shipper Program is 100 percent paper work", which tracks who shipped the product or the cargo, but not what is actually shipped as cargo. According to a TSA study, documents can easily be counterfeited, which increases the chances of claiming known shipper status fraudulently.[272] There is no mechanism to deter terrorists from tampering with air cargo while in transit from the shipper to the air carrier. While points vulnerable to tampering in air cargo transportation are lower than that of maritime cargo, the number of casualties in a bomb attack can exceed that of a dirty bomb and may add another financial burden on the crippling airline industry.

The Senate already passed a bill to improve air cargo security and eventually increase the inspection rate to 100%, however the bill has not been reviewed and did not pass. Congressmen Edward J. Market (D-MA) and Christopher Shays (R-CT) have recently attempted to pass another bill to increase air cargo screening. Congressman Edward J. Market says "We know that Al Qaeda continues to put aircraft near the top of its terrorist list. The cargo loophole presents a dangerous opportunity for terrorists." [273] However, TSA believes that 100% inspection policy is not technologically and financially feasible even when it's restricted to cargo

[267] GAO Report, GAO-06-76, "Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security", 17 October 2005.

[268] Information on types of inspection exempt cargo is considered sensitive.

[269] Ken Leiser, "Pilots Warn of Cargo Planes' Vulnerability to Attacks", St. Louis Post-Dispatch, 16 June 2002.

[270] Ken Leiser, "Gaps in Air Cargo Security May Offer Terrorism Openings Now, Few Packages are Screened for Explosives", St. Louis Post-Dispatch, 16 June 2002.

[271] "Plane Cargo Goes Unscreened", CBS News, 1 September 2004.

[272] Greg Schneider, "Terror Risk Cited for Cargo Carried on Passenger Jets; 2 Reports Cite Security Gaps", Washington Post, 10 June 2002.

[273] Frances Fiorino, "Cargo Screening Redux", Aviation Week & Space Technology, 9 May 2005.

on passenger aircraft.[274] This is the main motive behind development of a targeting system.

Air carriers and shippers also have concerns about %100 air cargo screening. Many believe that such a regulation will cripple the industry. UPS believes that enforcing the same screening requirements on cargo planes as passenger planes “make no sense”.[275] They believe that terrorists will have no incentives to blow up an air cargo plane and most of their aircraft has no doors that would enable an access from the cargo area to cockpit area, so terrorists cannot take over the plane hiding in a cargo container. An airline security analyst raised concerns about terrorists boarding air cargo planes undetected.[276] Further, terrorists may use air cargo planes to deliver dirty bombs in the United States. Some high value cargo shippers raised concerns about the risks that 100% screening would introduce regarding the integrity of their cargo. If sensitive cargo is not handled appropriately during screening, then there will be economic losses due to extra hazards on the shipment.[277]

CBP assumes the responsibility of targeting and inspecting international cargo at the US borders. CBP uses Automate Targeting System (ATS) that assigns a risk score to incoming cargo and then subjects high risk cargo to further inspection. To this end, CBP collects manifest information electronically through Air Automated Manifest System (Air AMS). Reporting of manifest information is required no later than 4 hours prior to flight’s arrival for most shipments. Cargo information on shipments originating from North America should be manifested before the aircraft leaves for US. Physical inspections and non-intrusive technology are employed for inspections. Air carriers importing cargo into the United States are eligible to participate in C-TPAT. Vulnerabilities in targeting of incoming cargo and C-TPAT program are discussed in Chapter 3.

Technology plays an important role in improving air cargo security. Using electronic seals that could make it more difficult to tamper with air cargo as well as placing global positioning systems and RFID tags that would increase transparency are among the possible solutions to reduce likelihood. However, as mentioned in Chapter 3, they won’t make cargo impenetrable. Blast hardened cargo containers offer a technology that would contain explosion and thus spread minimal damage. An important step would be to require that all cargo on passenger planes be carried on blast hardened cargo containers. 9/11 Commission calls for deployment of at least one hardened cargo container on every passenger aircraft. However, blast hardened containers are heavier, and this introduces extra fuel costs. According to a 1999 study, it would cost $125 million to cover the entire fleet with a single blast hardened cargo container.[278] Extra fuel costs would be $11 million. Further, such an asymmetric regulation will shift all air cargo from passenger aircraft to cargo aircraft.

Gore commission identified canine screening as the most effective tool to screen mails. It has proven to be effective in detecting agricultural products and drugs, and it has a potential to screen mail fast. Drawbacks of canine inspections include significant upkeep costs, failure to communicate the identity of the anomaly about the mail, need for a human handler and relatively brief periods of work.[279] For biological threats, detection technology is available and has been installed at several postal sites to detect anthrax. However, for most biological agents, detection technologies are still in development phase leaving postal system wide

[274] See Footnote 267.

[275] Joshua Levs, “Cargo Plane Security”, NPR, 8 April 2002.

[276] The same expert believes that a scenario where a terrorist hides in a cargo and takes over the plane is extremely unlikely.

[277] Angela Greiling Keane, “Insecurity Over Security”, Traffic World, 17 January 2005.

[278] National Materials Advisory Board, “Assessment of Technologies Deployed to Improve Aviation Security: First Report”, 1999.

[279] CRS Report to Congress, “Detection of Explosives on Airline Passengers: Recommendation of the 9/11 Commission and Related Issues”, 7 January 2005.

open to biological terrorism threat.

3. Passenger Identity Check

As the number of hijackings with fatalities soared in ‘80s, the need for passenger identity checks has dramatically increased. In 1998, a first version of a passenger prescreening system, known as Computer-Assisted Passenger Prescreening System (CAPPS), was developed and is still in use today. This system uses information on passenger itinerary to determine whether any further security check is needed on a passenger. The decision is made after information is checked against CAPPS rules which are a collection of behavioral rules and government’s watch list. Currently CAPPS prescreens 99 percent of passengers on domestic flights.

However, 9/11 showed clearly that terrorists can escape detection and get on board. Following ATSA requirements, TSA made an attempt to develop a second system called CAPPS II. The new system would feed new information into the decision about further security check. The system required name, date of birth, home address and phone number information, which would be checked against government databases after being verified with data that airline keeps about a passenger. Passengers with an unacceptable or unknown risk would not obtain a boarding card, and law enforcement agencies would be notified. However, the development of this program ended up in a failure when TSA canceled it in August 2004. TSA could not make the desired progress in resolving privacy issues, commercial and government data verification problems, and lack of international cooperation.[280]

Upon cancellation of CAPPS II development, TSA announced the development of a new prescreening program called Secure Flight. One of first radical changes of the new program is having TSA take over the prescreening responsibility from the air carriers; a change that could address the data incompatibility problems among different databases that system employs and guarantees easier access of government watch list data. At this stage, Secure Flight abandoned the CAPPS II goal to prescreen all passengers coming in and out of the United States, focusing only on developing a program to prescreen domestic passengers. Secure Flight seeks to prevent terrorists whose names are on Terrorist Screener Center’s database (TSC) from boarding the airplane. This database contains a larger set of names than the watch lists[281] previously maintained by FAA. Current CAPPS rules that help screening travelers with suspicious behavior and random selections for additional screening will not be abandoned. Both screening processes are required to identify those who may be terrorists and could evade watch lists. TSA plans to train passenger screeners on spotting potential terrorists using observational techniques known as Screening of Passengers by Observation Techniques (SPOT).

Development and implementation of Secure Flight has not been free of challenges. GAO released a report in March 2005 that identified key weaknesses in program development.[282] One of the key decisions is to identify the commercial data that should be collected by the air carriers. TSA has not decided which data should be collected by commercial airlines, how to transmit this data from air carriers and what kind of technology to use for name matching. TSA believes that commercial data will be useful to reduce false positives and negatives. Due to the use of commercial data, privacy still remains to be a concern with Secure Flight. Another problem with Secure Flight is the legal rights of those passengers who could be

[280] GAO Report, GAO-04-385, “Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges”, 13 February 2004.

[281] Prescreening was done against two separate lists named “No Fly” and “Automatic Selectee” before both of these lists were consolidated in TSC’s database in 2004.

[282] GAO Report, GAO-05-356, “Aviation Security: Secure Flight Development Under Way, But Risks Should Be Managed As System is Further Developed”, March 2005.

incorrectly denied boarding. It is not clear as how any false positive errors will be corrected.[283] Furthermore, Secure Flight is unable to detect identity theft. Thus, terrorists can still avoid detection as long as they keep a stolen identity. TSA failed to meet the timeline due to slow progress and concerns raised in March 2005 GAO report still remain to be addressed.[284] The report card released in December 2005 by 9/11 Commission assigned an F for the improvements in passenger pre-screening. As long as a better prescreening program replaces the current prescreening program that has been evaded on 9/11, passenger screening will be vulnerable.

European Union's privacy laws preclude air carriers from transmission of passenger data to TSA. European carriers have been reluctant to provide information about a traveler's destination and home address one hour before the take-off.[285] At this stage, Secure Flight leaves the prescreening responsibility of international travelers to CBP. However, TSA seeks to extend Secure Flight in the future to include international airline passengers. CBP prescreens most international passengers by subjecting them to visa requirements and screening their names against terrorist watch lists through Advanced Passenger Information System (APIS). One main problem is implementing APIS so far has been delays in transferring passenger information which resulted in boarding of suspected terrorists and diversion of their flights.[286]

Identity checks for those who need visa to enter the United States are performed under the US-VISIT program. The US-VISIT program uses biometric information to check the identity of international travelers. International travelers are granted visa if they have a valid reason to enter the United States and if their names do not appear on the watch lists. Biometric information guarantees that a traveler seeking entry into the United States is the same person as that person granted visa in a US consulate. The system is currently operational in 115 airports, 14 seaports and 154 land ports of entry in United States.

Success of the US-VISIT program rests on maintaining records in the watch lists up to date and effectiveness of law enforcement and intelligence agencies to correctly identify those who should be on the watch lists. CBP uses a system called IDENT to match fingerprints of those applying for visa and criminals on the watch lists. IDENT currently has fingerprints of at least 15,000 suspected terrorists and their alleged associates and over 1 million criminals and deportees overall. However, matching fingerprints may not ensure detection of a terrorist applying for a visa. Fingerprints can be modified.[287] Lawrence M. Wein of Stanford University said in Congressional Hearing last fall that probability of catching a terrorist on a watch list is 0.53 if he succeeds to modify his fingerprint.[288] Wein added "It would be naive to think that these people are not trying to defeat the system." Furthermore, depending on the quality of watch list database, fingerprint matches may result in incorrect results. Recently, it was discovered that due to a rare failure of an FBI fingerprint database one sex offender was released and killed four women in Georgia.[289] Another concern is the possible failure of the US consulate staff to detect fraudulent identity documents before granting visa. Training the US consulate staff on the interviewing process is crucial to deny entry to those who may not be on terrorist watch lists and seek entry into the United States by identity theft in a foreign country.[290]

[283] A passenger whose name is incorrectly matched against watch lists can fill Passenger Identity Verification Form to avoid future false positives. However, this process takes 45-60 days.
[284] GAO Testimony, GAO-06-374T, "Aviation Security: Significant Management Challenges May Adversely Affect Implementation of Transportation Security Administration's Secure Flight Program", 9 February 2006.
[285] Eric Lipton, "More European Air Data Sought by Security Chief", The New York Times, 20 May 2005.
[286] CRS Report to Congress, "Homeland Security: Air Passenger Prescreening and Counterterrorism", 4 March 2005.
[287] There are numerous web sites explaining what should be done to modify fingerprints.
[288] Robert O'Harrow Jr., and Scott Higham, "US Border Security at a Crossroads", 23 May 2005.
[289] "How Fingerprinting Systems Can Fail", NPR, 5 May 2005.
[290] GAO Testimony, GAO-03-1013T, "Border Security: New Policies and Increased Interagency Coordination Needed to Improve Visa Process", 15 July 2003.

As Secure Flight is not extended on international travelers, there is another security risk posed by the citizens of those countries that are involved in Visa Waiver Program. There are 27 overseas countries on the list, most of which are European countries. While European countries have struggled for years with local terrorist networks, they have continually overlooked the threat posed by radical groups in Europe. They maintained the belief that most of these radical groups were peacefully promoting ideas that they were not able express in their countries of origin due to lack of democracy. However after 9/11 attacks, Madrid and London bombings, most European countries came to realize that some radical groups are fostering violence and inspiring some to join global terrorist networks.

After Madrid bombing, Italy, France and Spain deported some of their legal residents allegedly threatening national security. Italian anti-terrorism expert Armando Spataro recently said in a conference at New York University that Italy is now a global crossroad of jihadi networks providing logistical support, particularly false documents.[291] A recent terrorist guideline found in Milano, Italy recommends recruits in Europe to avoid mosques and blend into social fabric. This strategy reduces the probability of detection in their home countries. Such European citizens have already been involved in radical terrorism. In 2003, a British citizen blew himself up in Tel Aviv killing three other people. As many Americans will remember, a French national, Zacarias Moussaoui was the only person in the United States prosecuted for involvement in 9/11 plot. All these suggest that Europe has been slow in realizing risks of harboring radical ideology. Thus, US officials have to act urgently to gather more data from their European counterparts. To this end, the United States has introduced a new requirement to incorporate biometric information in passports of those countries in the Visa Waiver Program. The first deadline that required issuance of passports with digital photographs has become effective as of October 26th, 2005. The deadline for installation of biometric chips has been extended to 2006.[292] However, as noted above, security breaches in biometric technology may enable potential terrorists in Europe to cross borders.

Another issue that split US government with its European counterparts is deployment of air marshals on international flights. Under the Federal Air Marshal Program, which has been significantly expanded after 9/11 to protect passengers, crew and aircraft from terrorist activities, air marshals are deployed in international flights of US air carriers. However, most European air carriers have refused boarding of federal air marshals.[293] On the other hand, Canada has initiated a training program for Royal Mounted Canadian Police to expand presence of armed police on aircraft. Air marshals could be key to reduce vulnerability to hijacking, and US should continue to seek cooperation from European governments to improve security on board.

In an effort to improve passenger identity checks, TSA is currently testing Registered Traveler Program which is expected to be fully implemented in 2006. The program is intended to reduce security screening for those travelers who voluntarily provide some personal information and allow background checks. Personal information includes name, address, phone number and date of birth. This program also collects biometric information through fingerprints. TSA recently announced that the program will use Smart Card technology that utilizes 10 fingerprints. Registered Traveler Program gained support from the industry because it is expected that more passengers will participate to eliminate inconveniences due to lengthy screening process. Privacy issues are raised as a potential drawback, but since the program is voluntary, privacy is less of a concern. TSA should not hesitate to introduce this program nationwide as it will help distribute resources from screening low risk passengers to high risk passengers. Registered Traveler Program does

[291] Sylvia Poggioli, "Europe's New Terror Policies Look Within", 10 October 2004.
[292] Chris Strohm, "Homeland Security Implements Rule of Digitized Passport Photos", Government Executive, 26 October 2005.
[293] Lufthansa is an exception.

not eliminate the primary screening. It eliminates the secondary screening. There are two risks in implementation of this program. First, those who sympathize with terrorists, but have not engaged in any criminal activity in the past, may be interested in getting registered traveler status. Second, identity theft is a potential problem as in all the other background and identity check systems.

We believe a good strategy would be to extend Registered Traveler Program at least to international travelers who are not already subject to visa requirements. This could help determine the low risk passengers among the foreign passengers who do not need visa to enter the United States. However, this approach may be subject to criticism particularly in Europe for discrimination.

4. Airport Security

Terrorists have used insider help to launch attacks on aircrafts in the past. Therefore, it is crucial to prevent criminals or terrorists getting a job in airports and have access to secure areas. TSA classifies nation’s airports into five categories (X, I, II, III and IV) based on the extent of air traffic and some special security considerations. Secured areas, security identification display areas (SIDA) and air operations areas (AOA) are closed for passenger access. These areas include baggage loading areas, near terminal buildings, and other areas close to aircraft parking areas such as air traffic control towers and runways used for landing and taking off. There are approximately 1,000,000 airport and vendor employees, 900,000 of which have duties in SIDA areas.[294] Currently, airports officials issue SIDA cards to grant unescorted access to airport workers, among which are aircraft mechanics, catering employees, cleaning crews, baggage and cargo loaders and refuelers.

All airport workers who have access to secure and sterile areas go thorough a criminal history check against TSA watch list. This procedure uses fingerprint information. According to a recent GAO study, among a random sample of 10 airports, 3 airports were discovered to employ workers granted unescorted access and have not gone through fingerprint based criminal history checks. For those workers who have escorted access, criminal history check is not a requirement. However, TSA is moving forward to request criminal history checks for all the workers in airports. Three problems will remain with fingerprint background checks. First, fingerprints are modifiable. Second, according to GAO, checks are made against federal databases, ignoring criminal history information in state and local databases. National security may suffer from a lack of a single database in the nation to check criminal history. Third, these databases do not have any information about the immigration status, leaving the system vulnerable to unauthorized access of illegal aliens who may not have any criminal history in United States.

Workers who have unescorted access rights enter secure areas using SIDA badges without being subject to any screening. TSA does not screen those workers as the procedure will require extra screeners and there will be extra passenger delays. Therefore, a worker who was granted unescorted access to sterile areas can introduce prohibited items or threat objects without screening. In a recent incident, Immigration and Customs Enforcement (ICE) arrested 14 illegal aliens in Boston Logan International Airport.[295] All illegal workers had temporary badges to access sterile areas and were working for a company providing janitorial services. TSA should impose random inspections for workers who have access to secure areas.

Prior to 9/11, GAO discovered security breaches on controls to access unescorted access to secure areas. GAO special agents were able to use fictitious law enforcement badges and credentials to access secure

[294] GAO Report, GAO-04-728, “Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls”, 4 June 2004.

[295] “ICE Arrests 14 Illegal Aliens Working at Logan Airport”, News release on ICE website, 25 March 2005.

areas, and walk unescorted to aircraft departure gates.[296] Two separate tests conducted before 9/11 demonstrated that the probability of unauthorized access increased over time. The first test conducted in 1995 at 19 busiest airports revealed that DOT inspectors successfully introduced fake bombs into the secure areas 40% of the time.[297] Three years later, DOT inspectors found out that an unauthorized person can gain access to secure areas 68% of the time.[298] These agents were issued tickets and boarding passes and could easily introduce threat objects into an aircraft. Similarly, workers with unescorted access to secure areas can help introduce threat objects on an aircraft. While details about how both these tests were not provided, it is very likely that probability of unauthorized access increases as the tests become more realistic.

It is critical to improve controls for secure area entry. Some improvements were made to improve through Airport Improvement Program (AIP) funds. Part of AIP funds were used to install computerized access controls, closed-circuit television to monitor secure areas and motion sensors which could reduce the likelihood of unauthorized access. However, there is still room for improvement. According to DOT test results from 2000, the probability of unauthorized access is still more than 0.3. Most of these tests were carried out in busiest airports in United States. There is no publicly available data on access controls at smaller airports. To improve access control, TSA is developing TWIC incorporating biometric information for those workers granted unescorted access to secure areas. However, as mentioned in Chapter 3, the progress in this program has been rather slow, leaving secure areas vulnerable to unauthorized access.

Air cargo facilities are exposed to similar security risks. Breaches in access control of cargo operations areas and lack of security training for facility workers are the main vulnerabilities in physical security of air cargo facilities.[299] Comprehensive background checks, which are required by ATSA, are another critical factor to minimize access control risks. In 1994, an off-duty Federal Express flight engineer made an unsuccessful attempt to hijack a Fed-Ex aircraft and crash it to company headquarters in Memphis. This incident is a grim reminder of how personnel with criminal tendencies can easily defeat the security system.

5. General Aviation and Border Air Traffic Control

Private aircraft could be weapons for suicide missions like any other aircraft as in 2002 Tampa skyscraper incident. Most general aviation airports are broadly accessible and located at isolated areas. Since 9/11, physical security improvements have been made at many airports through installation of fencing, lightning, surveillance cameras, and electronic access control gates.[300] Besides, many aircraft owners and airport managers have initiated “airport watch” programs seeking to increase awareness of security issues and follow relatively simple security measures that will prevent unauthorized aircraft use. However, these countermeasures have not been applied uniformly over all the general aviation airports in the United States, leaving some of the airports vulnerable to terrorism. Due to lax security measures, 70 aircraft were stolen from general aviation airports in United States between 1998 and 2003.[301] Other security improvements include background checks conducted by TSA on non-citizen student pilots as required in ATSA and flight restriction around some of the nation’s icons as well as critical infrastructure.

[296] GAO Testimony, GAO-04-232T, “Aviation Security: Efforts to Measure Effectiveness and Address Changes”, 5 November 2003.
[297] Max H. Bazerman and Michael D. Watkins, “Predictable Surprises”, Boston: Harvard Business School Press, 2004.
[298] GAO Testimony, GAO-01-1165T, “Aviation Security: Weaknesses in Airport Security and Options for Assigning Screening Responsibilities”, 21 September 2001.
[299] CRS Report to Congress, “Air Cargo Security”, 13 January 2005.
[300] GAO Report, GAO-05-144, “General Aviation Security: Increased Federal Oversight is Needed but Continued Partnership with the Private Sector is Critical to Long-Term Success”, 10 November 2004.
[301] GAO Testimony GAO-04-232T, “Aviation Security: Efforts to Measure Effectiveness and Address Challenges”, 5 November 2003.

These domestic improvements in general aviation security do not insure the nation against unauthorized access to airspace by small aircraft from Canada or Mexico. American airspace is vulnerable to intrusion originating beyond the borders. Awareness of loopholes in general aviation security has increased in Canada since 9/11, but their efforts seem to lag behind. Aviation Security Advisory Committee (ASAC) Working Group has recently reviewed air transportation security in Canada and recommended that general aviation security measures for flight schools and airports be considered for adoption in Canada.[302] For instance, international students do not have to go through background checks as required in United States for admission to Canadian flight schools. Consular officials have an option to review the criminal history of an applicant seeking to get a Canadian student visa and stay for more than six months, but this is not a mandatory requirement. Most general aviation security measures in United States can be used as an upper benchmark to make inferences about what the security risk in Canada is. Given that there are loopholes in general aviation security in United States, terrorists make exploit similar and in some instances more apparent vulnerabilities in Canada to launch suicidal attacks on urban areas or critical infrastructure close to northern borders. Ongoing partnerships with Canada that promote intelligence sharing should be expanded to cover updates on threats in both nations.

GAO has consistently reported on the nation's vulnerability of southwestern borders to air smuggling in late '80s and '90s. Drug smugglers either land illegally or airdrop the illegal contraband after crossing the borders. While this form of smuggling does not constitute a significant portion of drug smuggling across the nation's southwestern borders, concerns remain regarding potential failure to detect private aircraft intrusions into US airspace. In 1987, GAO reported that[303], some drug traffickers build a record of legal activity across the borders to reduce the likelihood of inspections, or using the airdrop option before landing and going through normal Customs procedures. Air smuggling is still used heavily as means to transport illegal contraband in Central America[304], and is still a threat that is encountered by Customs and other law enforcement agencies.[305]

FAA maintains radar coverage for US airspace. These radars provide consistent coverage for over 90% of the airspace at high altitudes. However, radar coverage at lower altitudes faces problems at mountainous and distant terrain. Air smugglers have eluded interdiction using these vulnerabilities of radar coverage.[306] CBP uses its aviation resources to intercept aircraft that may not appear on radar, or verify of the identity of the aircraft that is spotted on the radar screen. Observing the flight patterns, Customs can identify suspicious aircraft and may choose to intercept the aircraft. However, in the areas where there is high volume of traffic, tracking of suspicious activity is difficult. FAA is currently implementing a modernization program to improve air traffic systems. Most of the improvements will be to manage commercial air traffic around major airports.

Another risk that may jeopardize the performance of air traffic control is a cyber attack on the nation's air traffic control system. Security procedures to prevent illegal access to computer systems should be in place to minimize this risk. Background checks of employees working at airport traffic control centers and

[302] A complete set of recommendations can be found on http://www.tc.gc.ca/vigilance/sep/recommendations.htm.

[303] GAO Report, GAO/GGD-87-91, "Drug Smuggling: Large Amounts of Illegal Drugs Not Seized by Federal Authorities", June 1987.

[304] Statement of Michael A. Braun, Chief of Operations Drug Enforcement Administration Before the House International Relations Committee Subcommittee on Western Hemisphere, November 9, 2005 "The Illicit Drug Transit Zone in Central America." Also see GAO Report, GAO/NSIAD-94-233, "Drug Smuggling: Interdiction Efforts in Central America Have Had Little Impact on the Flow of Drugs.", 2 August 1994.

[305] Congressional testimony on drug trafficking in the southwest by John C. Varone in 2001.

[306] Mike Gallagher, "US Customs Beaten at the Border", Albuquerque Journal, 24 October 1995.

establishing physical security measures in and around the facilities are necessary. We will not elaborate more on cyber security risks as their discussion is beyond the scope of this report.

VI. CONCLUSIONS

Terrorists have variety of options to strike the US homeland. Rifles, shoulder-fired missiles and nuclear material are highly proliferated in the world black market. They have the skill to develop powerful explosives, are ready to sacrifice their lives in suicidal attacks and have the persistence to exploit every point of vulnerability along US borders. They can introduce their operatives as the land borders are so porous; bring weapons in, as many deadly types of weapons are cheap, light and can easily fit in golf bag or a car trunk[307]; launch attacks on critical targets exploiting multiple security gaps. This report sought to identify potential pathways to introduce illegal aliens and weapons into the United States, and the conclusion is that we have a long way to go for ideal security.

Before the Iraqi war, FBI believed that approximately 2000 MANPADS were on the arms black market. However, supply of these missiles has increased as most of Iraqi war arsenal is still unaccounted for. FBI estimates this number around 4000.[308] US officials in Iraq have made an attempt to collect those weapons for $500[309]; a strategy doomed for failure as the minimum offered for shoulder-fired missiles is $5,000.[310] Most low-end models of these portable weapons are easy to acquire as they have highly proliferated across the globe. For instance, at least 40 countries are believed to own RPG in their arsenal, 27 terrorist groups are believed to possess at least one type of shoulder-fired missiles. [311] Terrorists have already used this relatively new arsenal against civilian and military targets.[312] According to FBI, in 2002, 29 planes had been hit by these weapons, mostly in the third world countries. In addition to this figure would be potential threats by US adversary states supporting terrorist organizations ready to attack US economic interests globally.

Dirty bombs and other forms of radiological bombs are among the threats that we may confront in the near future. According to International Atomic Energy Agency (IAEA), illicit trafficking of radioactive material has recorded 182 incidents involving nuclear material, 330 incidents involving radioactive material other than nuclear, 23 incidents involving both nuclear and other radioactive material and 5 incidents involving other material between 1993 and December 2003. According to GAO, material smuggled in a significant number of these cases could be used to produce a nuclear weapon or a dirty bomb.[313] There are a variety of ways to smuggle nuclear material through borders: they can be hidden in a car, shipped in a container, carried in a personal luggage through an airport, or simply carried while walking through the border undetected. Recently, one man carrying a hidden radioactive material through the Sheremetyevo Airport in Moscow in a briefcase was captured.[314] An overwhelming majority of these confirmed cases would help produce dirty bombs. However, as shown in Figure 26, there are 10 incidents with high enriched uranium which is used in nuclear weapon development.

[307] Tom Zeller, “Cheap and Lethal”, The New York Times, 26 October 2003.

[308] Thom Shanker, “Cash-and-carry Missiles in Iraq”, The New York Times, 24 April 2005.

[309] Josh Tyrangiel, “How Secure are the Skies?”, Times, 25 August 2003.

[310] Philip Shenon, “US Reaches Deal to Limit Transfers of Portable Missiles”, 21 October 2003.

[311] Among the major terrorist organizations thought to possess shoulder-fire missiles are Revolutionary Armed Forces of Colombia (Colombia), Al Qaeda (Middle East), National Liberation Army (Colombia), Armed Islamic Group (Algeria), Hizbul Mujahedeen (Kashmir), Liberation Tigers of Tamil Eelam (Sri Lanka), Kurdistan Workers Party-PKK (Turkey), Hezbollah (Lebanon), Oromo Liberation Front (Ethiopia), United Somali Congress (Somali), National Union for Total Independence of Angola (Angola), Various Rebel Groups (Congo), Chechen Rebels (Russia), Taliban (Afghanistan), United Wa State Army (Myanmar). From Tom Zeller’s article in footnote 195.

[312] For instance, a comprehensive overview of shoulder-fired missiles threats on aviation is given in Terry O’Sullivan, “External terrorist threats to civilian airliners: A summary risk analysis of MANPADS, other ballistic weapons risks, future threats, and possible countermeasures policies”, CREATE, 14 April 2005.

[313] GAO Report, GAO-03-15, “Combating Terrorism: Actions Needed to Improve Force Protection for DOD Deployments through Domestic Seaports”, 22 October 2002.

[314] C.J. Shivers, “Keeping That Special Glow Safe at Home”, The New York Times, 1 May 2005.

Figure 26 Distribution of Incidents Involving Nuclear Material, 1993-2003[315]

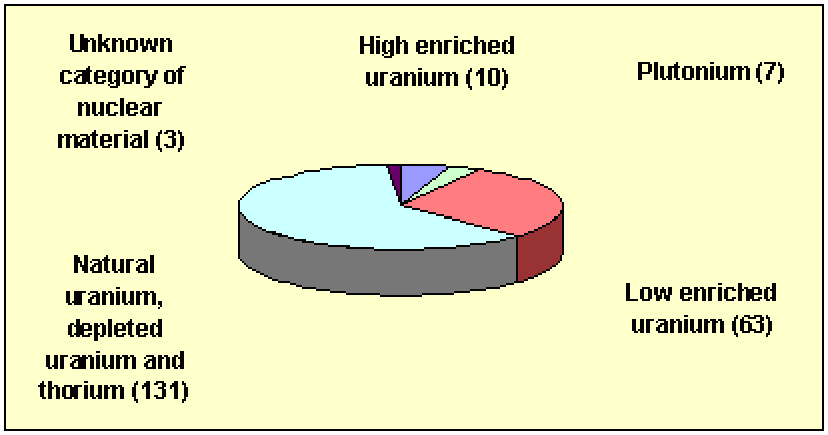
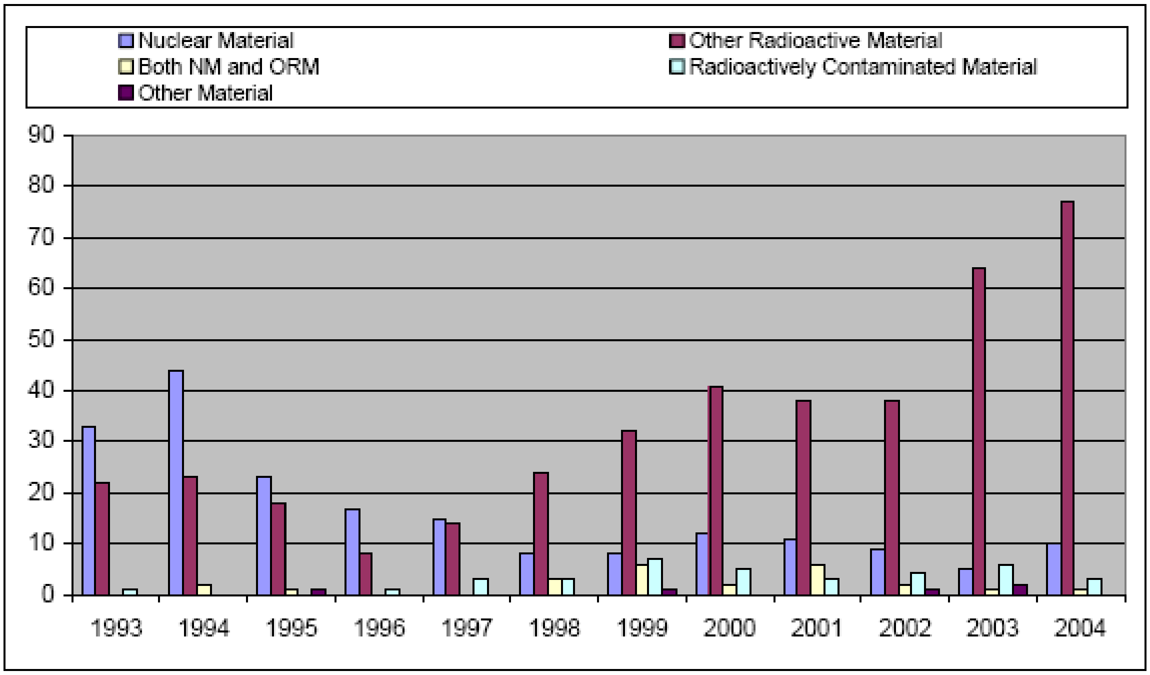


Figure 27 Incidents Confirmed in 1993-2004[316]



Building a nuclear bomb is not a trivial task and terrorists do not have the technology to build one. However, nuclear weapon production is no longer a monopoly, as many other developing nations are building nuclear bombs. There is no guarantee that developing nations will provide nuclear weapons to terrorist groups with a similar political agenda. The recent Abdel Qader Khan, top Pakistani nuclear scientist, case elevates fears of nuclear weapon smuggling. The United States is currently helping some 30 countries to detect nuclear materials at their borders. Russia, with almost 12,500 miles of borders surrounded by politically unstable countries is on the top of list of nations with nuclear material black market. As long as there is no global solution to proliferation of nuclear material, it will rank as one of the top threats in cross-border terrorism.

[315] Source: www.iaea.org.
[316] Source: www.iaea.org.

In general, most threats target critical facilities along US borders. Therefore, we need to develop the capabilities to detect threats before they actually reach the homeland. To this end, C-TPAT and CSI serve for a very critical mission. As mentioned earlier, both initiatives fail to address intermodal transportation security in both countries. We have to realize that if a nuclear or radiological bomb arrives at our border, it may be too late to act. For instance, terrorists could detonate a dirty bomb in a container using a GPS reader right after arrival at the port, leaving very little time for detection. Similarly, terrorists do not have to detonate a nuclear bomb in the heart of Manhattan; they can take over a ship, preferably with hazardous cargo, and blow everything up as they get sufficiently close to the shores. Whether a terrorist group would use such a precious weapon in a rather less effective way is another question. However, either of the two scenarios could cause enough harm to radically change the way Americans are used to living.

Further cooperation is needed from other nations trading with the United States. Intelligence sharing, improving homeland security in other nations, developing common strategies to fight organized crime, contraband smuggling, terrorism and drugs and accordingly more secure trade are among the benefits of partnerships. To this end, US has recently announced one such partnership with Canada and Mexico, called Security and Prosperity Partnership (SPP). This partnership has the potential to achieve what CSI currently does not; developing transportation security in these two bordering countries in an attempt to reduce the probability of a threat object reach the ports of entries. CSI should be extended to embrace this objective. The awareness of transportation security is rising in Europe after Madrid train and London subway attacks. However, the focus is more to beef up passenger transportation security as opposed to cargo transportation security. Furthermore, the government may create incentives for companies that trade with those countries partnering with the United States to this end.

Better technology and more human expertise are needed. Technology should reduce dependence on human intervention in screening and detection. Passenger screening at most airports is subject to human errors because many screeners are inexperienced and there is a high level of attrition. Making airport screening job an attractive one is a tough task. Rather, we need to invest in new technologies that will minimize the need for human capital at any airport. However, at the maritime borders, we need more people, more experience to detect the anomalies in trade patterns. Government has to develop a better understanding of how maritime trade works. This is particularly important as it is not economically feasible to inspect %100 of the cargo. More expertise will help pick the right cargo for inspection. We need both more people and better technology along land borders. The northern borders are especially vulnerable to terrorist crossing because the Border Patrol's border coverage is way lower than in the southwestern border, and it is harder to detect humans crossing in the forest areas. Furthermore, US waterways cannot be left unguarded. The Coast Guard's equipment shortage should be quickly addressed before terrorists exploit this vulnerability.

In conclusion, terrorists are far more sophisticated than they were during the cold war. They are committed to harm people and US economic interests. Borders should be secure enough to deter terrorists from launching attacks. Total elimination of the risk is not possible. Therefore, a systems based risk management approach is required to allocate limited resources to fight terrorism appropriately. Consequences of a failure may be catastrophic. We need to move faster to close the security gaps without disrupting trade; making borders impenetrable for adversaries and wide open for friends.