

**The Effectiveness and Economic Impact of Enhancing Container Security**

By

**Eric L. Dresser**

B.S. Marine Engineering Systems  
United States Merchant Marine Academy, 2003

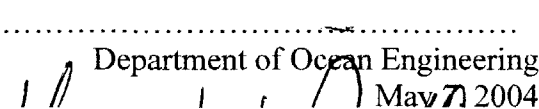
Submitted to the Department of Ocean Engineering  
in Partial Fulfillment of the Requirements for the Degree of  
Master of Science in Ocean Systems Management

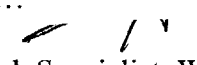
at the  
Massachusetts Institute of Technology

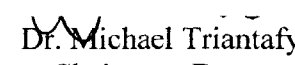
June 2004

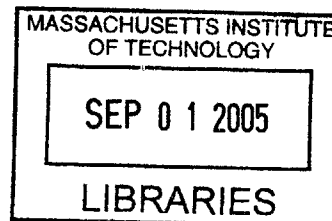
© Eric L. Dresser, MMIV. All rights reserved

The author hereby grants MIT permission to reproduce and to  
distribute publicly paper and electronic copies of this thesis document in whole or in part.

Signature of Author.....  
 Department of Ocean Engineering  
May 27 2004

Certified by.....  
 Dr. Hauke Kite-Powell  
Research Specialist, Woods Hole Oceanographic Institution  
Lecturer, Department of Ocean Engineering  
Thesis Supervisor

Accepted by.....  
 Dr. Michael Triantafyllou, Professor of Ocean Engineering  
Chairman, Department Committee on Graduate Students



**BARKER**

Page Intentionally Left Blank

# **The Effectiveness and Economic Impact of Enhancing Container Security**

by

Eric L. Dresser

Submitted to the Department of Ocean Engineering in Partial Fulfillment  
of the Requirements for the Degree of

Master of Science in Ocean Systems Management

## **ABSTRACT**

Over the past few decades, international containerized shipping has evolved to become the main artery of global trade, providing both convenient and inexpensive access to goods from markets around the world. Yet the very size and efficiencies that have made container shipping such an attractive means of transport have also created a system that is highly vulnerable to terrorist exploitation.

This paper outlines the current initiatives taken by both the public and private sector to address the security vulnerabilities in the container industry. The solution targets three main areas for security: documentation/information, physical security, and inspections. The technology utilized to improve the physical security of the container can also be used to track shipments and secure the container from pilferage. This generates a win-win relationship between enhancing container security while improving supply chain information and control. An economic model is used to demonstrate the cost savings and cost avoidance from the information and control provided by security technologies. The savings to shippers more than offsets the cost of implementing these technologies. This is a valuable approach to solving the problem of container security because it concurrently provides incentive to the private sector and protects global interests.

Thesis Supervisor: Dr. Hauke Kite-Powell

Title: Research Specialist, Woods Hole Oceanographic Institution  
Lecturer, Department of Ocean Engineering

## **ACKNOWLEDGEMENTS**

This thesis would not have been possible without the assistance and support of Dr. Hauke Kite-Powell who has been extremely supportive with my research. I would like to thank Dr. Hank Marcus for providing me the opportunity to study at MIT. Furthermore, I would like to thank Michael Wolfe for his help and contribution to my research. Lastly, thanks go to my family and friends for their support while I have been at MIT. This thesis is dedicated to advancing the security and protecting the homeland of the United States. My thoughts and prayers will always be with the victims and their families of the horrific terrorist attacks on September 11, 2001.

## TABLE OF CONTENTS

<b>ABSTRACT.....</b>	<b>3</b>
<b>ACKNOWLEDGMENTS.....</b>	<b>4</b>
<b>TABLE OF CONTENTS.....</b>	<b>5</b>
<b>LIST OF FIGURES.....</b>	<b>7</b>
<b>LIST OF TABLES.....</b>	<b>8</b>
<b>NOMENCLATURE AND ACRONYMS.....</b>	<b>9</b>
<b>CHAPTER 1: INTRODUCTION.....</b>	<b>11</b>
PURPOSE.....	11
BACKGROUND.....	12
PROCEDURE.....	14
<b>CHAPTER 2: VULNERABILITY AND SECURITY DEMAND.....</b>	<b>16</b>
BACKGROUND.....	16
VULNERABILITY INVESTIGATION.....	19
POTENTIAL IMPLICATIONS.....	22
SUMMARY.....	24
<b>CHAPTER 3: CURRENT INITIATIVES.....</b>	<b>26</b>
BACKGROUND.....	26
GOVERNMENT REORGANIZATION.....	26
OPERATION SAFE COMMERCE.....	27
CONTAINER SECURITY INITIATIVE.....	31
CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM.....	34
PORT SECURITY GRANT PROGRAM.....	38
MARITIME TRANSPORTATION SECURITY ACT OF 2002.....	39
SMART AND SECURE TRADELANES.....	40
INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE.....	40
SUMMARY.....	42
<b>CHAPTER 4: CARGO CERTIFICATION AND DOCUMENTATION.....</b>	<b>45</b>
BACKGROUND.....	45
INFORMATION FILING.....	46
INFORMATION TIMING.....	48
DETAIL AND ACCURACY.....	48
AUTOMATED TARGETING SYSTEM.....	49
SUMMARY.....	50
<b>CHAPTER 5: PHYSICAL SECURITY.....</b>	<b>53</b>
BACKGROUND.....	53

THEFT.....	54
TECHNOLOGICAL ADVANTAGES.....	57
ELECTRONIC CARGO SEALS.....	58
SECURITY SENSORS.....	59
WIDE AREA COMMUNICATION AND TRACKING.....	60
INFORMATION SYSTEMS.....	61
TECHNOLOGY AVAILABLE.....	61
SUMMARY.....	63
<b>CHAPTER 6: INSPECTIONS.....</b>	<b>65</b>
BACKGROUND.....	65
NON-INTRUSIVE INSPECTION TECHNOLOGY.....	68
RADIATION DETECTION PAGERS.....	74
X-RAY INSPECTION SYSTEMS.....	75
GAMMA-RAY INSPECTION SYSTEMS.....	76
SUMMARY.....	78
<b>CHAPTER 7: ASSOCIATED COSTS.....</b>	<b>80</b>
BACKGROUND.....	80
INDIRECT SECONDARY IMPACTS: INCREASED INSPECTIONS.....	82
SMUGGLING AND THEFT LOSSES.....	84
DIRECT COSTS OF IMPLEMENTING TECHNOLOGY.....	88
ENHANCED EFFICIENCY SAVINGS.....	89
SUMMARY.....	90
<b>CHAPTER 8: CONCLUSION.....</b>	<b>92</b>
SUMMARY.....	92
RECOMMENDATIONS FOR FUTURE WORK.....	94
<b>WORKS CITED.....</b>	<b>96</b>
<b>WORKS CONSULTED.....</b>	<b>100</b>
<b>APPENDICES.....</b>	<b>102</b>

## LIST OF FIGURES

Figure 1 – Fifteen Pounds of Depleted Uranium.....	20
Figure 2 – Potential Economic Impact.....	24
Figure 3 – Container Supply Chain Vulnerabilities.....	25
Figure 4 – Information System Outline.....	50
Figure 5 – Common Container Security Seals.....	53
Figure 6 – Bolt Removal and Open Door Process.....	56
Figure 7 – Bolt Replacement and Touch-up Paint.....	56
Figure 8 – Example Satellite Communication Network.....	62
Figure 9 – NaviTag in the Field.....	63
Figure 10 – X-ray Image of a Fully Loaded, 40-foot Container.....	75
Figure 11 – Fixed-site, Rail-mounted Unit.....	77
Figure 12 – Mobile Unit.....	78
Figure 13 – Cost Savings Categories.....	88

## LIST OF TABLES

Table 1 – Boston, A Model Port Areas for Improvement.....	30
Table 2 – Top 10 Foreign Ports, by Number of U.S.-bound Containers, 2001.....	32
Table 3 – Top 10 U.S. Ports, by Number of U.S.-bound Containers, 2002.....	33
Table 4 – Status of C-TPAT Membership in 2003.....	38
Table 5 – Technology Characteristics.....	72
Table 6 – Technology Functionality Matrix.....	73
Table 7 – Cost of Implementing a Tracking Network.....	83
Table 8 – Potential Benefits of Enhanced Efficiency.....	90



## **NOMENCLATURE AND ACRONYMS**

ACS: Automated Commercial System

ADS: Automatic Dependent Surveillance

AES: Automated Export System

APEC: Asia Pacific Economic Cooperation

ATS: Automated Targeting System

BEST: Bangkok Laem Chabang Efficient and Secure Trade

CFR: Code of Federal Regulations

CIA: Central Intelligence Agency

CSI: Container Security Initiative

C-TPAT: Customs – Trade Partnership Against Terrorism

DC: Distribution Center

DHS: Department of Homeland Security

DOT: Department of Transportation

FBI: Federal Bureau of Investigation

FEU: Forty Equivalent Unit

FY: Fiscal Year

GPS: Global Positioning System

ILWU: International Longshore and Warehouse Union

IMO: International Maritime Organization

ISO: International Organization for Standardization

ISPS: International Ship and Port Facility Security Code

LNG: Liquefied Natural Gas

MARAD: Maritime Administration

MTSA: Marine Transportation Security Act of 2002

NII: Non-Intrusive Inspection

NVOCC: Non-Vessel Operating Common Carriers

OSC: Operation Safe Commerce

PFNA: Pulsed Fast Neutron Analysis

PSGP: Port Security Grant Program

RFID: Radio Frequency Identification

SOLAS: Safety of Life at Sea

SST: Smart and Secure Tradelanes

STAR: Secure Trade in the APEC Region

TEU: Twenty Equivalent Unit

TSA: Transportation Security Administration

USCBP: United States Customs and Border Protection

VACIS: Vehicle and Cargo Inspection System

WMD: Weapons of Mass Destruction

WSC: World Shipping Council

## CHAPTER 1: INTRODUCTION

### **Purpose**

The terrorist attacks of September 11, 2001 have had a major impact on the overall security of the United States. Specifically, supply chain security has become a primary focus due to its vulnerability and global implications. The United States has 95,000 miles of open shoreline, 361 ports, and a 3.5 million square mile exclusive economic zone. Shipboard containers make up 95% of the cargo tonnage moving in and out of the country. Each year, more than 7,500 commercial vessels make approximately 51,000 port calls, unloading over 7 million marine containers. According to the U.S. Department of Commerce, container cargo will quadruple in the next 20 years to approximately 30 million containers per year (Williscroft 2003).

Such conditions constitute an open invitation to terrorists around the world, who are rapidly gaining access to extremely dangerous weapons and materials. The Brookings Institution has estimated that if one of these containers housed a Weapon of Mass Destruction (WMD) it would have the potential to kill up to one million people. The secondary impacts would be catastrophic as well. It is likely that the ensuing panic would force the closure of other U.S. ports and hamper trade for years. The Institution forecast that the financial impact of such an event would exceed \$1 trillion (Davey 2002).

Robert Bonner, U.S. Customs Commissioner, best summarized the goal in a speech given shortly after the attacks: “We must reaffirm the importance of knowing your customer and consider the overall ‘air-tightness’ of your supply chain, from factory floor,

to loading dock, to transportation to our border. Every single link in that chain must be made more secure against the terrorist threat.”

Therefore, this thesis has four primary goals:

1. To provide a current look at the container sector of the transportation industry and the inherent vulnerabilities.
2. To introduce and examine the current security initiatives and programs to address these vulnerabilities.
3. To study the practical solutions and the challenges of implementing them.
4. To demonstrate the win-win relationship between enhancing container security while improving supply chain information and control.

## **Background**

In response to this challenge, several legislative and industry initiatives have been launched over the past two years including the creation of the Transportation Security Administration (TSA), the Customs-Trade Partnership Against Terrorism (C-TPAT), the U.S. Customs Container Security Initiative (CSI), and the Smart and Secure Tradelane Initiative (SST).

Many indirect costs and secondary impacts have hit the container industry due to the terrorist attacks and the implemented heightened security over the past two years. Trade security becomes more critical as each supply chain becomes increasingly distributed and global. Not surprisingly, the early adopters of trade security programs are multi-billion dollar corporations that have a global presence and depend on the “frictionless” flow of goods and information. The charter members of C-TPAT, for

example, include General Motors, Ford, Daimler-Chrysler, Target Corporation, Motorola, BP America, and Sara Lee.

Arguably, the primary driving force behind trade security is money. The investment required to create a more secure supply chain is easily justified when compared to the costs associated with experiencing longer, unpredictable lead-times or acute disruptions. Among other things, these costs come in the form of (ARC 2002):

- Additional inventory
- Slowing or shutting down production lines
- Lost revenue due to stock-outs or missed promotions
- Longer cash-to-cash cycles
- Higher insurance rates
- Increased transportation costs (e.g. more expedited shipments)

For a multi-billion dollar company, these costs can exceed hundreds of millions of dollars. Simply stated, the financial impact of supply chain disruptions is felt by everyone, from suppliers to end-consumers.

There is currently a tremendous amount of work being done in exploring the issues of supply chain security and its economic impact on various groups. For the companies which offer carrier services there is great potential for valuable knowledge, transparency, and reliability due to tracking and security. These benefits can be offered through a number of different electronic means.

The cost of this type of off-the-shelf technology such as radio frequency identification (RFID) tags, global positioning systems (GPS), electronic seals (e-seals),

readers, and signposts and the capital required to implement them is currently, relatively high. With increased production, time, and competition the cost of these devices will decline. There is also the possibility that legislation could intervene and mandate a certain amount of accountability or security verification for each container. In the airline industry, each person pays a ten dollar security fee for every plane ticket purchased. A similar scheme could be implemented for the container industry. For example, the government could collect a security fee per container and use it to subsidize security equipment and U.S. Customs' efforts used throughout the world. On the other hand, there are several different areas in which there is a potential for cost savings to the carriers and to individual companies who install these tracking devices and as a result have the ability to operate a more efficient supply chain.

From a different perspective, if a terrorist attack were to occur, the devastation on the global economy and on global supply chains could be disastrous. No one would lose more than the carrier companies themselves. Tradelanes and shipping ports could be gridlocked or even shut down for an overwhelming amount of time. This is another incentive to invest in these new technologies to help automate and secure the world's supply chain.

### **Procedure**

This discussion will begin with a review of the vulnerability of the container industry. There is a high demand throughout the country to protect us from another terrorist attack and to specifically secure the millions of containers which enter our country

each year. The possible consequences of a container attack could be disastrous and paralyzing to our economy. The resonating effects of such an attack will also be explored.

Then, the current initiatives and response which has already been taken over the past two and a half years will be introduced and their approach to the overall solution will be described.

Once the vulnerability and current approaches have been presented, the solution will be explored through the three most critical areas of the container security industry:

1. Cargo Certification and Documentation
2. Physical Security
3. Inspections

These areas will be explored while discussing the impact of their solutions and the challenges that each aspect exemplifies.

Finally, there will be a study of the economic impacts due to enhanced security. A win-win template will be presented, which shows the benefits in supply chain management that are incurred when container security and visibility are improved.

## CHAPTER 2: VULNERABILITY AND SECURITY DEMAND

### Background

Prior to the attacks on September 11, 2001, supply chain security concerns were primarily focused on controlling theft, and reducing contraband such as illegal drugs, illegal immigrants, and the export of stolen products. Supply chain security fell within the jurisdiction of the Department of Transportation (DOT).

As a result of these attacks, the United States sustained an enormous economic and societal disruption. The possibility of another attack rippled through every facet of our economy. Security has become a top concern and a primary focus for both the public and private sectors. Future terrorists are inspired by the seeming ease with which America could be attacked and encouraged by the devastating blow that is delivered through such actions. Not only is loss of life their target, but also the economic and public psyche effects which accompany an attack.

“On September 11<sup>th</sup>, we observed nineteen men wielding box-cutters force the United States to do to itself, what no adversary could ever accomplish: a successful blockade of the U.S. economy. If a surprise terrorist attack were to happen tomorrow involving sea, rail, or truck transportation systems that carry millions of tons of trade to the United States each day, the response would likely be the same self-imposed global embargo. Trade security should be a global priority; the system for moving goods affordably and reliably around the world is ripe for exploitation and vulnerable to mass disruption by terrorists (Flynn 2003).”

In the United States there are 361 ports, 95,000 miles of coastline, 25,000 miles of navigable waterways, 4,000,000 miles of exclusive economic zone. Over 200 million containers move through ports throughout the world each year. World Shipping Council



(WSC) estimates underscore the magnitude of the potential problem: approximately 800 oceangoing liners and their multinational crews make more than 22,000 port calls in the United States each year. Consisting primarily of container ships and roll-on/roll-off vessels, these liners from every part of the globe deliver to the United States approximately 7.8 million containers of imported cargo per year – an average of 20,000 containers per day – and these numbers are growing dramatically (Koch 2002).

At the Los Angeles-Long Beach port complex, for example, one of the nation's largest and busiest port facilities, officials estimate that port traffic will double over the next two decades. The planned mile-long wharfs will accommodate up to six new generation cargo vessels with the capacity to carry as many as 15,000 containers. Dozens of computerized cranes will offload these containers onto endless lines of 18-wheelers and hundreds of trains (Sahagun 2002).

The container industry is a system designed for high efficiency and rapid transit through the logistics system. However, it is not an industry designed for security. Speed and cost are the motivating force behind the industry's explosive growth and sustained success. There are no economic incentives to inspect the cargo or to generate additional paperwork beyond what is necessary to move containers through the various steps in the supply chain. The huge volume of containers entering into the U.S. everyday, and the typically lax controls over cargo packing provide ample opportunities to introduce a weapon into a container at several points within the transportation process. Prior to September 11<sup>th</sup>, only 2% of all containers entering the U.S. were being inspected. Unless

some vast changes are made to the current system in place, a weapon could easily transit through a U.S. port undetected.

An attack on a U.S. port would cause serious economic damage, but the threat is not restricted to just the ports. From the port, containers are transported throughout the country on an expansive logistics network including truck, rail, and inland waterways. Several thousand containers move along major transportation routes daily, thus exposing numerous urban centers and facilities such as nuclear power plants, chemical and oil refineries, hazardous material storage sites, and key transportation infrastructure to an attack (Binnendijk 2002). Along the Houston Ship Channel, for example, there are 150 such sites that may be vulnerable (Hollings 2001).

A terrorist could use a simple mechanical triggering device or even more sophisticated technology based on a global positioning system (GPS). Suddenly, intermodal containers have become potential weapon delivery systems, a “poor man’s” missile. Using advanced technology, a number of containers, perhaps arriving on opposite coasts, might be configured to attack selected targets in different parts of the country with near simultaneity. Weapons delivered by such means would put at risk a large number of lives, significant infrastructure, public and business confidence, trade, and prosperity. Potentially, an attack of this nature could shut down global trade for a prolonged period of time.

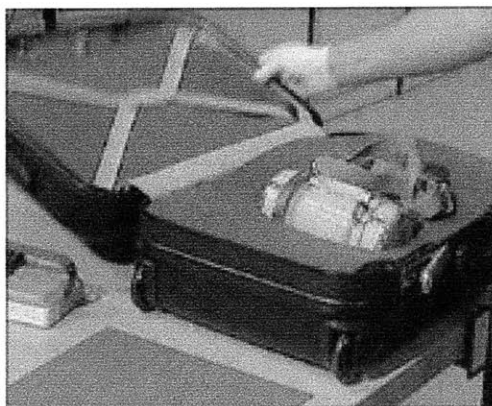
The characteristics of a specific container threat are based on the type of weapon that might be employed, the probability that terrorists would have access to their weapon of choice, and the likelihood of using a seaborne container as the means of delivery. The container itself seems ideally suited for mounting a terrorist attack. The abundant cargo space of the international standard 8-foot-by-8-foot

container, which ranges in length from 20 to 48 feet, and most commonly found in 40 foot lengths, affords a convenient vehicle to convey both large devices, in which the container itself may be part of the weapon. Furthermore, small concealed devices intended for receipt and use by an agent in country could be hidden within a shipment of goods. Thus, nuclear, radiological, and large conventional explosive devices could be employed as well as chemical, biological, or smaller conventional devices (Binnendijk 2002).

### **Vulnerability Investigation**

ABC News conducted an investigation in July of 2002 to see if American authorities could stop the shipment of radioactive material. The test demonstrated important shortcomings in the Customs' screening process. On July 4, 2002, in a train station in Europe, a suitcase containing fifteen pounds of depleted uranium, shielded by a steel pipe with lead lining, began a secret 25-day, seven-country journey. Its destination was the United States.

It was the kind of uranium that, if highly enriched, would, by some estimates, provide about half the material required for a crude nuclear device and more than enough for a so-called "dirty bomb". The depleted uranium packed in the suitcase, as shown in Figure 1, was not highly enriched and therefore not dangerous, but similar in many other key respects. In other words, to the human eye or to an x-ray scanner, the depleted uranium would look similar to an actual radioactive shipment.



**Figure 1 – Fifteen pounds of depleted uranium shielded by a steel pipe with a lead lining (Ross 2003).**

Starting in Austria on July 4<sup>th</sup>, the suitcase began its journey by rail, traveling first across the border to Hungary, where the passengers' passports were checked, but there was no inspection of the suitcase. From there, it was on to Romania, through the Transylvania Alps, across the fields of Bulgaria and into Turkey, all without even one inspection of the suitcase. This is precisely the route and the method authorities say has been used in the past to transport radioactive material smuggled out of the former Soviet Union.

Throughout the 47-hour European rail trip, the suitcase, packed with depleted uranium, sat untouched on a rack in the cabin. There was no evidence of radiation detectors in use anywhere.

The suitcase traveled all the way to Istanbul, Turkey, which is considered a hub of the world's nuclear black market. Dr. Fritz Steinhausler, of Stanford University in California and the University of Salzburg in Austria, an expert in weapons trafficking who has compiled a database of nuclear-smuggling incidents, described it as "a crossroad between a leaking Central Asian region and possibly a receptive Middle East".

Turkish authorities report they have detected more than 100 cases of such attempted smuggling in the last few years. The investigating team was doing what some law enforcement officials say al Qaeda terrorists have known how to do for years. Documents in Arabic seized from one of Usama Bin Laden's top aides five years ago show he apparently planned to use shipping containers packed with sesame seeds as part of a plan to smuggle high-grade radioactive material into the United States.

Hours after the investigating team's arrival in Istanbul, the suitcase of radioactive material was prepared for shipment by sea to the United States. The suitcase was placed inside an ornamental Turkish chest that was carefully marked as containing depleted uranium, in case inspectors discovered it. Then, in the middle of a busy Istanbul street, the chest itself was crated and nailed shut. The crate containing the suitcase was then nestled alongside crates of huge vases and Turkish horse carts in a large metal shipping container that was ordered from a company that arranges shipments to the United States.

The company hired to handle the shipping did not know, nor did its workers check to see, what was inside the crate. The container, with the suitcase inside, left Istanbul on July 10<sup>th</sup>, bound for the Port of New York, where U.S. Customs Service officials have very publicly claimed they have made huge improvements to prevent anything radioactive from getting through.

At 2 a.m. on July 29<sup>th</sup>, the ship carrying this suitcase cleared the Verrazano Bridge and entered New York Harbor. At this point, no one had asked a single question about what was in the container. A weapon smuggled in this way could be armed in advance and ready to fire, using the ship as the delivery device. The ship carrying the container was

tied up at the Staten Island dock in New York, where the Customs officials have claimed that there is a state-of-the-art system in place to detect even a small, low-level amount of radioactive material.

Although the shipping container holding the suitcase was selected by Customs for additional screening, it sailed right through the inspection and left the port without ever being opened by Customs inspectors. A few days after its arrival in the United States, the container was on the back of a truck headed for New York City.

Finally, the container was taken to a New York Port Authority warehouse on Pier No. 1, just across the river from lower Manhattan, at the foot of the Brooklyn Bridge. When the crate was pulled out, it was easy to see it had never been opened since leaving Istanbul. Port Authority police are assigned to this warehouse facility, but there are no radiation detectors there and no one asked about the unusual shipment in a container full of Turkish horse carts. This investigative test demonstrated many important shortcomings of the Customs' screening process and the security of the entire supply chain one year after the attacks on September 11<sup>th</sup> (Ross 2003).

### **Potential Implications**

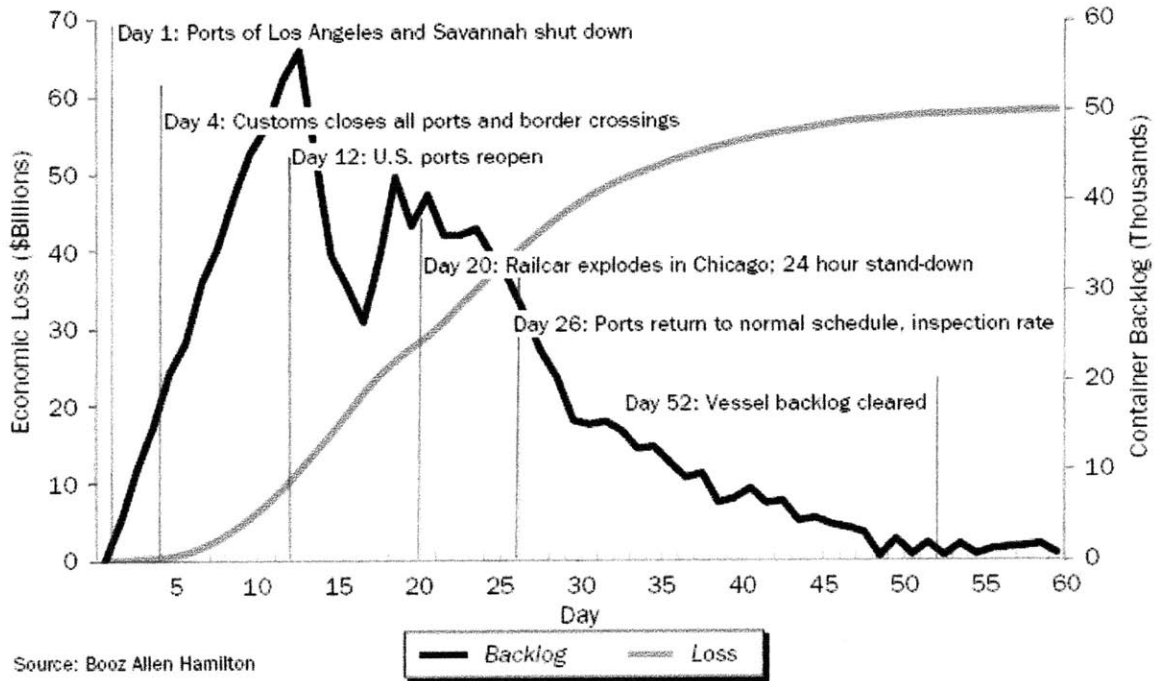
The effects of an attack through the use of a shipping container would greatly depend on the type of weapon used and the location of such an attack. However, one thing is certain: if a container were used as a means of attacking the United States, all ports in the U.S. would shut down for an indefinite period of time. The economic impact of such an incident would be far reaching and extremely devastating.

On October 1, 2002, the International Longshore and Warehouse Union (ILWU) representing nearly 11,000 dockworkers on the west coast went on strike. Every port on the West Coast was idled by a bitter, escalating contract feud between shipping companies and dockworkers that had enormous effects on the national economy. Not only were 11,000 dockworkers forced off their jobs, but 29 ports from San Diego to Seattle were paralyzed during their busiest time of the year. Giant cranes that lift cargo containers from docked ships did not move. Containers filled with an array of merchandise were not opened. In a time when more and more companies rely upon Just-in-Time (JIT) logistics to replenish their warehouses as well as reduce inventories and safety stocks, the stoppage in shipments was even more overwhelming.

The strike lasted eleven days, before President George W. Bush ended it with a court order based upon the Taft-Hartley Act. It was estimated that each day the ports on the west coast were shut down it cost the American economy over \$1 billion per day. By the time the longshoremen resumed work, the damage to the economy was nearly \$20 billion (Rosynsky 2002).

The U.S. economy is based on a free flow of goods. All businesses, big or small, rely in some manner upon movement of goods through the world's logistic systems. Various experts have estimated that the cost to the U.S. economy of port closures due to the discovery or detonation of WMDs could be significant. For example, in May 2002, the Brookings Institution estimated that costs associated with U.S. port closures resulting from a detonated WMD could amount to \$1 trillion (O'Hanlon 2002). Estimating the cost of discovering an undetonated WMD at a U.S. seaport, as shown in Figure 2, Booz, Allen and

Hamilton reported in October 2002 that a 12-day closure would cost approximately \$58 billion (Gerencser 2002)

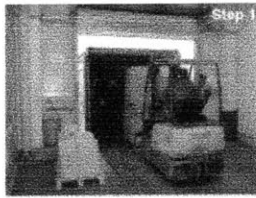


**Figure 2 – Potential Economic Impact (Gerencser 2002)**

### Summary

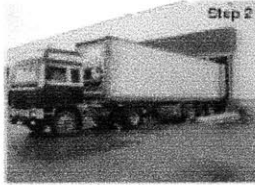
Over the past few decades, international containerized shipping has evolved to become the main artery of global trade, providing both convenient and inexpensive access to goods from markets around the world. Yet the very size and efficiencies that have made container shipping such an attractive means of transport have also created a system that is highly vulnerable to terrorist exploitation. Figure 3 helps outline a few of the numerous steps in a supply chain and some points of potential vulnerability.





**Overseas warehouse loading a container for export**

**Potential vulnerability:** Warehouse facilities may have weak controls and personnel practices. For example, access to shipping areas may not be secure and warehouse personnel practices may lack sufficient background checks. Also, seals attached to containers may provide minimum security against tampering.



**Contracted trucking company preparing to leave warehouse for port terminal**

**Potential vulnerability:** Visibility of in-transit activities may not be apparent to the trucking company or the supplier. The location of the truck and container may not be known or tracked. Furthermore, truck drivers may have broad discretion over their routes, which are subject to last minute changes.



**Port terminal receives container and stages it for vessel loading**

**Potential vulnerability:** Terminal operators may not adequately screen employees for criminal backgrounds. Some containers may be at risk for tampering because the container may sit for extended periods before being staged and loaded on a cargo ship.



**Ocean carrier loads container for trans-oceanic voyage**

**Potential vulnerability:** Containers might not have a seal or show signs of tampering. The ocean carrier and terminal operator may not routinely check containers for seals or signs of container tampering prior to or during the loading of the container on the ship.



**Ocean carrier en-route to multiple ports**

**Potential vulnerability:** Container ship may make multiple stops at various seaports to unload and load containers. The container ship transits through various routes and ports posing different levels of security risks.

**Figure 3 – Container Supply Chain Vulnerabilities (GAO 2003)**

Unless fundamental changes in the practices of the current system are introduced, the possibility of seaborne container terrorism will remain a significant threat. However, proposals to alter current container shipping business practices must balance security concerns with economic imperatives, lest global commerce be severely disrupted.

These are the implications and the extent to which the container industry affects the U.S. economy and our day-to-day life. It is clear that something must be done to help secure this industry and prevent terrorists from using it as a means of attacking our homeland.

## **CHAPTER 3: CURRENT INITIATIVES**

### **Background**

In response to the obvious vulnerability of the container industry to a terrorist attack, many changes have been made within the U.S. government, and a number of different initiatives have been launched to address this problem and develop a practical solution. Right now, none of these initiatives has changed the intermodal transportation environment sufficiently to fundamentally reduce the vulnerability of the cargo container as a means of terrorism. However, all are important advances for building an effective risk management approach to container security. This is a good foundation which simply did not exist prior to September 11, 2001.

### **Government Reorganization**

The first reform introduced by the government addressing transportation security, following September 11<sup>th</sup>, was the signing of the Aviation and Transportation Security Act on November 19, 2001. The Act created the Transportation Security Administration (TSA), which initially was part of the DOT. Furthermore, on November 25, 2002 President George W. Bush signed the Homeland Security Act of 2002. This was a major reform and reorganization attempting to unite the many different agencies which work towards the security of the United States into one department known as The Department of Homeland Security (DHS). In terms of container security, the United States Coast Guard (USCG) and TSA were both moved from the DOT to the newly created DHS.

## **Operation Safe Commerce (OSC)**

In February of 2002, Operation Safe Commerce (OSC) was initiated as a private-public partnership in the New England area. This project examined end-to-end supply chain security for a containerized shipment entering the Northeastern United States from Eastern Europe. The project identified potential supply chain security weaknesses. The first phase of the project focused on the safety of the New England region serving as a prototype test of cargo container security issues that could have a worldwide application. Using ideas developed by former USCG Commander Stephen Flynn, Ph.D., the theory of OSC is to push back the borders of the U.S. for cargo container security purposes to the shipping containers' point of origin overseas. The goal of the program is to provide security while not impeding international commerce.

Commercially available technology was chosen to track and monitor a test container from Slovakia to Hillsborough, New Hampshire. Electronic monitoring devices were installed at five locations along the route of travel. A GPS transceiver and data logger, seal, and intrusion detection device were also installed on the container itself. The container was then loaded from the Osram Sylvania plant in Nove Zamky, Slovakia to the Osram Sylvania plant in Hillsborough, New Hampshire.

The purpose of the tracking technology is to make sure the container is not diverted from its trip to its intended destination. The purpose of the intrusion detection device is to make sure that no one opens the container to insert weapons or other items that may be a potential threat to national security. The project identified many, major, potential supply chain security weaknesses within their current conveyance, physical, and procedural

security practices. The detailed results and conclusions are unavailable due to their sensitivity. However, the proposed solutions were all aimed at improving visibility and control throughout the entire chain. Therefore, due to the initial results of OSC Phase I, OSC Phase II was launched in November of 2002.

OSC Phase II includes federal, state, and local governments, along with industry partners all collaborating on the security initiative. Congress, through the 2002 Supplemental Appropriations Act, provided \$28 million in funding for OSC Phase II to improve the security of container shipments through pilot projects involving the United States' three largest container ports of entry, Los Angeles/Long Beach, New York/New Jersey, and Seattle/Tacoma. Projects consist of representation from all components of the supply chain, including ports and their feeder locations, overseas customers and port partners, and the shipping lines serving these locations (Steigman 2002).

Eighteen projects have been selected for OSC Phase II, which focus on container supply chain security shortcomings, from the point of origin to the point of destination. They examine technologies and practices while testing innovative solutions in an operational environment. The projects scrutinize supply chain security through container tracking and tracing technology, non-intrusive detection strategies, and improved seal concepts. Only off-the-shelf technologies were utilized for the studies.

One of several OSC Phase II projects currently underway across the U.S. is known as "Boston – A Model Port". This initiative is examined in more depth due to available, unclassified information as well as its small-scale resemblance of container ports across the country.

This initiative has brought together various federal, state, local, and industry representatives with a stake in maintaining an effective maritime transportation system in and around Boston, Massachusetts. The initiative has garnered executive level support and participation from important government and political leaders, including USCG District Commander, the Mayor of Boston, Boston's Police and Fire Commissioners, the Port Director for Customs, the Director of Massachusetts' Office of Commonwealth Security, the Director of Massachusetts Emergency Management Agency, and other important officials. The overall goal of the initiative is to enhance port and transportation security while facilitating commerce. The concept for the "Boston – A Model Port" initiative was developed over several months during the early part of 2002. From April 2002 to October 2002, the work groups met on numerous occasions, ultimately determining a baseline security assessment and then identifying areas for improvement.

The container work group, led by U.S. Customs and Border Protection (USCBP), was focused on developing security measures and supply chain efficiencies to be employed in handling, transferring, storing, and transporting of containers through the Port of Boston. P.W. Conley Terminal is Boston's only container terminal, located in South Boston directly across the Reserved Channel from the Black Falcon Cruise Ship Terminal. The number of imported containers averages 3,000 per month while exports average 1,000 per month. The terminal receives feeder services from Halifax, Nova Scotia and New York City weekly, container ships from Europe and Asia, and services approximately 200 container vessels per year (OSC 2003).

Positive Findings and Progress Made:

- U.S. Customs has dedicated two X-ray trucks in Boston. Typically a very high percentage (100% of targeted containers and on the order of 60% of all remaining containers) are screened as they are offloaded at the terminal
  - Note: The Automated Targeting System (ATS) is constantly being refined by Customs, but the most recent reports indicate that 5.4% of containers are targeted by ATS (Koch 2004)
- Held demonstration at Conley terminal to familiarize all group members with containers, terminology, and the X-ray truck. Planning for container vessel familiarization tour for the same purpose
- U.S. Customs has received new technology – radiation isotope detectors, telescopic cameras, that will assist in positive and rapid identification of potential weapons of mass destruction (WMD) sources
- U.S. Customs and USCG developing offshore intercept/evaluation of specified containers targeted under the automated targeting system (ATS)
- U.S. Customs has the ability to obtain information on any given container at any time

**Table 1 – Boston, A Model Port Areas for Improvement (OSC 2003)**

<u>Areas For Improvement</u>	<u>Method</u>	<u>Notes</u>
Need a container stripping facility on the seaport terminal to avoid “dangerous” containers being transported through populated areas to stripping facility	Build stripping facility at Conley Terminal	Requires Funding
Seal verification is not always an effective way to ensure container has not been accessed (can get in w/o breaking the seal)	-Find other ways to assure integrity -Don't rely on seals	
Need to track history of containers themselves beyond last few port calls	Obtain shipping company equipment tracking records	Beyond requirements of Customs' national initiatives like CSI, C-TPAT, etc.
Export container screening	Install fixed x-ray or detection system at gate	Requires funding; traffic flow issues
All agencies w/ container jurisdiction should be educated on all container related programs	Conduct Multi-Agency strike force operation/awareness session	
Need contingency plan for when anomaly detected in a container (radiation, etc.) prior to installing any type of fixed device	Work with consequence management group	
At sea container inspection w/ new technologies	Develop CG/Customs at-sea interception capability	Need criteria; commerce flow issues
Point of Origin foreign facility security assessment for container vessels	TBD – Work with U.S. Customs to assess container facilities overseas	Focus on Canada first

The “Boston – A Model Port” study was an effective approach to addressing security needs. Not only did the study raise the level of security in Boston’s port, but it created a set of best practices which can be used as a benchmark for the rest of the country.

### **Container Security Initiative (CSI)**

The Container Security Initiative (CSI) has been another highly funded project to address security issues. The general goal, very much like OSC, is to enhance container security without impeding the free flow of goods. CSI represents a true paradigm shift by changing the focus of inspection from the arrival port to the loading port. The result is to identify and intercept dangerous cargo and improve cooperation among our key trade partners in advancing this vital agenda. CSI consists of four core elements (Ridge 2003):

1. Identifying “high-risk” containers, through the use of advance information, before they are loaded on board vessels destined for America. This cargo includes containers that may conceal – based on intelligence and risk-targeting principles – terrorist weapons...or even terrorists.
2. Pre-screening the “high-risk” containers at the foreign CSI port before they are shipped to the U.S.
3. Using detection technology to pre-screen high-risk containers, including both radiation detectors and large-scale x-ray-type imaging equipment, so that the security inspection can be done quickly without slowing down the flow of legitimate cargo.
4. Using smarter, “tamper-evident” containers – containers at the port of arrival that indicate to USCBP officers whether cargo has been tampered with after security screening overseas.

A critical element in the success of this program will be the availability of advance information to perform sophisticated targeting. CSI is meaningless unless the risk assessment can be accomplished by an inspector in a loading port. That data must arrive in time for an inspector to analyze it and to follow up on any questions that may arise. The U.S. Customs’ new “24 hour rule”, requiring the submittal of a cargo manifest one day

prior to loading in a foreign port, will help provide additional time to gather this information and process it.

CSI was launched in January of 2002 by the USCBP. As a first step, USCBP determined the top 10 “mega-ports”, see Table 2, that send containers to the U.S., and contacted the governments in these locations to solicit their participation in the CSI. The locations were identified based on their volume of sea container traffic destined for the U.S.; however, the CSI approach should not be restricted to only these locations. Risk assessments and trade analysis will play an important part in future deployments, and increased security measures are vital to the operations of any port in today’s environment.

Table 3 shows the U.S. top 10 ports for importing containers.

**Table 2 – Top 10 Foreign Ports, by Number of U.S.-bound Containers, 2001 (GAO 2003)**

Foreign ports	Number of U.S.-bound containers	Percentage of total containerized U.S.-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	5.0
Bremerhaven, Germany	256,500	4.5
Tokyo, Japan	159,600	2.8
Genoa, Italy	119,700	2.1
Yantian, China	114,000	2.0
<b>Total (top 10 ports)</b>	<b>2,764,500</b>	<b>48.5</b>



**Table 3 – Top 10 U.S. Ports, by Number of U.S.-bound Containers, 2002 (GAO 2003)**

U.S. ports	Number of U.S.-bound containers	Percentage of total containerized U.S.-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	4.0
Tacoma	273,000	3.8
Oakland	268,000	3.7
Houston	233,000	3.3
<b>Total (top 10)</b>	<b>6,241,000</b>	<b>87.0</b>

Today, the top 20 ports account for 68% of all cargo containers arriving at U.S. seaports. Through July of 2003, the Commissioner of CSI, Robert Bonner, had successfully enlisted nineteen of the twenty busiest ports in the world to participate in CSI. Additionally, to be eligible for CSI, ports must meet the minimum standards for the program. That is, they have to have the detection equipment, the capacity, and the will to implement CSI with USCBP and DHS.

CSI involves stationing USCBP officers at foreign seaports to do the actual targeting and identification of “high-risk” containers. The basic premise is to extend the zone of security outward, so that American seaports and borders become the last line of defense, not the first. The country can ill afford to focus exclusively on domestic ports.

According to Customs officials, the most important benefits of CSI derive from the collocation of U.S. Customs officials with foreign customs officials (GAO 2003). Prior to the implementation of CSI, Customs officials in U.S. ports screened container data using the ATS and inspected “high-risk” containers on their arrival in the United States. With

the placement of officials overseas, Customs expects that the added value of real-time information sharing will improve Customs' ability to target "high-risk" containers. For example, using the ATS, U.S. Customs officials may identify unfamiliar consignees that have been flagged as "high-risk" but are later determined not to be high risk based on the host customs' knowledge and experiences. Customs' presence overseas is intended to help ensure that containers identified as "high-risk" are inspected prior to arrival in the United States. In addition, Customs hopes that the collocation of its officials with foreign customs officials will result in relationships that enhance cooperation and intelligence sharing (GAO 2003).

The screening at CSI ports will in most cases take place during "down time" while containers wait at the port terminal prior to being loaded onto vessels. Therefore, Customs officials believe that CSI should facilitate the flow of trade to the United States and could reduce the processing time for certain shipments. In addition, CSI eliminates the necessity of inspecting containers for security purposes, absent additional information affecting their risk analyses, when they reach the United States. CSI also offers benefits to foreign ports that participate in the program, including deterrence of terrorists that may target their ports and a shorter time frame to resume operations in the event of a catastrophic incident (GAO 2003).

### **Customs-Trade Partnership Against Terrorism (C-TPAT)**

As CSI is used to push the borders of the U.S. outwards to foreign ports, the Customs-Trade Partnership Against Terrorism (C-TPAT) is an initiative geared towards securing the entire supply chain, end-to-end. C-TPAT is a joint government-business

initiative that builds cooperative relationships, which strengthen overall supply chain and border security. C-TPAT recognizes that Customs can provide the highest level of security only through close cooperation with the ultimate owners of the supply chain, importers, carriers, brokers, warehouse operators, and manufacturers. Through this initiative, Customs requires businesses to ensure the integrity of their security practices and communicate their security guidelines to their business partners within the supply chain (USCBP 2002).

Businesses must apply to participate in C-TPAT. Participants must sign an agreement that commits them to the set guidelines and procedures. A comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by Customs and the trade community must be conducted. The assessment addresses the areas of procedural security, physical security, personnel security, education and training, access controls, manifest procedures, and conveyance security. A supply chain security questionnaire must be submitted to Customs. A program to enhance security throughout the supply chain in accordance to C-TPAT guidelines must be developed and implemented. Finally, the C-TPAT guidelines must be communicated to other companies in the supply chain and work must be done toward building the guidelines into relationships with these companies.

The C-TPAT validation process guidelines, provided in Appendix A, as written and upheld by USCBP are specific to each segment in the supply chain including importers, brokers, manufacturers, warehouses, air carriers, sea carriers, land carriers, air freight

consolidators, ocean transportation intermediaries, and non-vessel operating common carriers (NVOCC).

C-TPAT offers businesses an opportunity to play an active role in the war against terrorism. By participating in this first worldwide supply chain security initiative, companies will ensure a more secure supply chain for their employees, suppliers, and customers. Beyond these essential security benefits, Customs will offer additional potential benefits to C-TPAT members which include some of the following (USCBP 2002):

- A reduced number of inspections (reduced border times)
- An assigned account manager (if one is not already assigned)
- For current Low-Risk Importers, an opportunity to expand “low-risk” treatment to all divisions within the company
- Access to the C-TPAT membership list
- Eligibility for account-based processes (bimonthly/monthly payments, e.g.)
- An emphasis on self-policing, not Customs verifications
- Eligibility for participation in other Customs programs
- General benefits of enhanced security, which may in the future reduce certain insurance and/or bond policies

Perhaps more importantly participants also avoid the consequences that may occur if they do not “volunteer”. Such non-participation will likely result in classification of the importer into an “unknown” security category, and accordingly the chances increase for:

- Higher scrutiny of cargo
- Increased reviews and audits
- Added examinations
- Requests for information
- No guarantees for cargo processing times

Every U.S. importer, distributor, customs’ broker, carrier, and manufacturer is eligible to become a C-TPAT member. According to C-TPAT officials, in January of 2003, approximately 1,700 companies had signed C-TPAT agreements, which allowed

them to become C-TPAT members and receive the benefits of a partially reduced risk score. During the first year of the program, more than 800 of these companies had completed the next step in the program and submitted security profiles to Customs. Customs sent feedback letters to 429 companies, granting 416 of them full program benefits, including a further reduction in their company risk scores. The remaining thirteen companies received feedback letters from Customs informing them that their profiles were insufficient for the companies to be granted full benefits. The table below provides information on the status of the C-TPAT program members by type of industry sector and state of key program elements (GAO 2003).

By May of 2003, as outlined in Table 4, the number of agreements signed nearly doubled to 3,355. According to C-TPAT officials, the program's staff was able to review all 1,837 security profiles and prepare all 1,105 feedback letters in a timely manner. Customs has not removed any companies from C-TPAT membership due to the determination that a member company's commitment is not serious or that a member company had intentionally misled Customs or for any other matter. As of the end of May of 2003, Customs had not fully implemented other critical program elements, such as validations, company action plans, and annual assessments designed to ensure that companies have taken action to improve and maintain supply chain security practices. A few validations had been completed, as the concept was being pre-tested.

**Table 4 – Status of C-TPAT Membership in 2003 by Industry and Program Elements (GAO 2003)**

Key program elements	Importers		Carriers		Brokers, freight forwarders, nonvessel operating common carriers		Domestic port authorities and terminal operators		Total	
	Jan.	May	Jan.	May	Jan.	May	Jan.	May	Jan.	May
	Agreements signed	1,106	2,119	134	410	466	806	0	20	1,706
Security profiles submitted to Customs	517	1,088	88	242	254	499	0	8	859	1,837
Feedback letters sent by Customs	306	623	37	163	86	312	0	7	429	1,105
Validations (pretested)	0	15	0	0	0	0	0	0	0	15
Action plans	0	0	0	0	0	0	0	0	0	0
Annual assessments	0	0	0	0	0	0	0	0	0	0

**Port Security Grant Program (PSGP)**

The Port Security Grant Program (PSGP) funds security planning and projects to improve dockside and perimeter security. The latest round of TSA grants have been awarded to 199 state and local governments, and private companies for a total of \$170 million (Appendix B). These new awards will contribute to important security upgrades such as new patrol boats in the harbor, surveillance equipment at roads and bridges, and the construction of new command and control facilities. TSA, the USCG, and the DOT's Maritime Administration (MARAD) evaluated the PSGP applications and selected grant award recipients. In 2002, \$92 million was awarded in the first round of port security grants.

In addition to the \$170 million, DHS also provided \$75 million in port security grants for specific projects from the fiscal year (FY) of 2003 supplemental budget. The funds will be distributed by the Office for Domestic Preparedness to cover recent infrastructure security protective measures, security enhancements, training, exercises, equipment, planning, and information sharing (Ridge 2003). See Appendix B for additional information on funding.

## **Maritime Transportation Security Act of 2002 (MTSA)**

The Maritime Transportation Security Act of 2002 (P.L. 107-295) (MTSA) was enacted by the U.S. Congress on November 25, 2002. MTSA amends the Merchant Marine Act of 1936 to “establish a program of greater security for United States seaports, and for other purposes.” Congress, in enacting MTSA, noted the pivotal role of ports in the economy of the United States, the difficulties inherent in attempting to secure the nation’s port and intermodal transportation system, the vulnerabilities of that system to acts of terrorism, and the diverse types of federal crimes that are committed in the port environment (Congress 2002).

Some of the key features of MTSA are as follows:

- Requirements for port, facility, and vessel vulnerability assessments
- Preparation by the Secretary of Transportation of a National Maritime Transportation Security Plan and area plans for each U.S. Coast Guard Captain of the Port Zone
- Development of security plans for certain facilities and commercial vessels
- The issuance and use of Transportation Security Cards for personnel whose responsibilities require them to access secure spaces aboard ships
- Establishment of a permanent program of grants to facilitate the enhancement of maritime security
- Assessment by the Secretary of Transportation of the effectiveness of antiterrorism measures at foreign ports
- Establishment of an enhanced system of foreign seafarer identification
- Creation of Maritime Security Advisory Committees at national and area levels
- Installation and operation of Automatic Identification Systems aboard certain commercial vessels
- Establishment of a program to better secure international intermodal transportation systems, to include cargo screening, tracking, physical security, compliance monitoring, and related issues.
- Provision of civil penalties for violation of statutes or regulations
- Extension of seaward jurisdiction of the Espionage Act of 1917 to twelve nautical miles offshore of the territorial sea baseline
- Codification of the U.S. Coast Guard Sea Marshal program and consideration of utilizing merchant mariners and other personnel to assist the Coast Guard

- Requirements that shipment data be provided electronically to U.S. Customs prior to arrival or departure of cargo
- Reporting by the Secretary of Transportation to Congress on foreign-flag vessels calling at United States ports
- Development of standards and curriculum for maritime security professional training

### **Smart and Secure Trade Lane (SST)**

Launched by the Strategic Council on Security Technology, the Smart and Secure Trade Lanes Initiative (SST) is an industry-driven, supply chain security initiative. The SST initiative focuses on deploying an end-to-end supply chain security solution, from point of origin to point of delivery, across multiple global trade lanes.

Recognized as the world's most comprehensive and practical security initiative for the intermodal cargo community, SST incorporates new, more secure, business practices and advanced technologies with over 65 partners such as terminal operators, carriers, service providers, and shippers in a global information network for intermodal container security.

SST participants are committed to taking an aggressive and innovative approach to complying with international government requirements while improving security, productivity, and efficiency. SST is rapidly expanding throughout Europe, Asia, and North America. Most importantly, SST enables global ports to drive a new generation of security-based programs worldwide (SST 2003).

### **International Ship and Port Facility Security Code (ISPS)**

The International Maritime Organization's (IMO) Diplomatic Conference of December of 2002 adopted new regulations to enhance maritime security through



amendments to Safety of Life at Sea (SOLAS) Chapters V and XI. Chapter XI, previously covering ship safety has been split into two new chapters, XI-1 and XI-2.

Chapter XI-1, Special Measures to Enhance Maritime Safety, has been enhanced to include additional requirements covering ship identification numbers and carriage of a Continuous Synopsis Record.

Chapter XI-2, Special Measures to Enhance Maritime Security, has been created and includes a requirement for ships and companies to comply with the International Ship and Port Facility Security (ISPS) Code. The ISPS Code contains two parts. Part A is mandatory, while Part B is recommendatory and contains guidance for implementation of the code. The USCG has decreed that sections of Part B of the code will also be taken into consideration. Chapter XI-2 also sets out requirements for ship security alert systems and control and compliance measures for port states and contracting governments.

As well as the new regulations in SOLAS Chapter XI-2, the Diplomatic Conference has adopted amendments to extant SOLAS regulations accelerating the implementation of the requirement to fit automatic identification systems (AIS). The Diplomatic Conference has also adopted a number of conference resolutions including technical cooperation, and the cooperative work with the International Labor Organization and World Customs Organization.

Some of the new provisions regarding maritime security may be required on completion of the work of these two organizations. These requirements form a framework through which ships and port facilities can cooperate to detect and deter acts which pose a threat to maritime security. The regulatory provisions do not extend to the actual response

to security incidents or to any necessary clear-up activities after such an incident (Lloyds 2002).

In summary the ISPS Code:

- enables the detection and deterrence of security threats within an international framework
- establishes roles and responsibilities
- enables collection and exchange of security information
- provides a methodology for assessing security
- ensures that adequate security measures are in place

It requires ship and port facility staff to:

- gather and assess information
- maintain communication protocols
- restrict access; prevent the introduction of unauthorized weapons, etc.
- provide the means to raise alarms
- put in place vessel and port security plans; and ensure training and drills are conducted

**Summary**

In conclusion, there is currently a lot of funding and researching aimed at improving the vulnerabilities of the container industry and the supply chains which support it. The major initiatives and legislation has been outlined in this chapter. However, there are more legislative and other efforts to try to improve security through any possible means. For example, in February of 2004, the U.S. and Liberia signed a landmark pact allowing the U.S. Navy to search Liberian ships in international waters. This type of accord is expected to become a model as the U.S. seeks other two-country deals authorizing searches on the high seas (AP 2004).

C-TPAT is a commendable first step toward improving container security by encouraging greater awareness and self-policing among the private sector participants most

directly involved with shipping, receiving, and handling containerized cargo. Its current weakness is the nearly complete absence of Customs personnel to monitor the level of compliance among the C-TPAT participants. This lack of auditing ability creates the risk that if a terrorist incident involves a C-TPAT participant, the entire program would be discredited since Customs would have no grounds to suggest why other participants did not also pose a similar risk. Enough resources must be committed to allow Customs to put in place a “trust, but verify” system accompanied with regular recertification protocol.

CSI is an important program because it is leading the way for change in the inspection process from the focus of inspection on the arrival port to the loading port. Similar to C-TPAT, there are extremely serious resource implications associated with making this an effective system. As of March of 2003, U.S. Customs had only twenty inspectors assigned overseas to support this initiative (Flynn 2003). In order to be effective, CSI must be fully implemented globally, and that would require the equivalent of a diplomatic service.

OSC is the most promising initiative towards advancing a comprehensive and credible approach to container security. It not only builds on C-TPAT and CSI, but it takes container security to the next level by building a greater understanding of the current vulnerabilities within a variety of global supply chains, and it ensures that new technology and business practices that are designed to enhance container security are both commercially viable and successful. OSC will be of little value if common performance based standards are not developed that can be quickly adopted and adequately enforced

within the global transportation and logistics community. There must not be a competitive disadvantage for taking steps to serve broader public interests.

Overall the programs and initiatives thus far have been successful for a couple of reasons. First, they have brought a lot of attention and funding to address the problem of container security. Due to the extensive work and studies currently focused on container security, both the public and private sectors have begun to realize their importance. A number of private companies have been developing and testing their own technology to help solve this problem, while other companies have been actively involved in securing their supply chains. The early adopters of trade security programs are multi-billion dollar corporations that have a global presence and depend on the “frictionless” flow of goods and information. The charter members of C-TPAT, for example, include General Motors, Ford, Daimler-Chrysler, Target Corporation, Motorola, BP America, and Sara Lee.

Second, these initiatives serve as pilot programs to test equipment, develop industry best practices, and explore all possible solutions in search of the most efficient and effective way to enhance container security. These tests have been effective in discovering both the strengths and weaknesses of the world’s current logistics systems and identifying the critical points where visibility and control are critical. The continued work and results achieved by these studies will facilitate a more secure industry.

## CHAPTER 4: CARGO CERTIFICATION AND DOCUMENTATION

### Background

Beyond these Customs' initiatives, enhanced container security requires a clearly defined and coordinated government information system capable of receiving, analyzing and acting on data determined by the government to be necessary to screen shipments. Whenever a container is shipped into the U.S. there are a number of documents which must accompany the shipment. Several parties are involved with the documentation including the importer, shipper, steamship operators, freight forwarders, Customs, customs' brokers, banks, and consolidators. A few of these documents include (Lanier 2002):

- Shipper's Export Declaration
- Commercial Invoice
- Certificate of Origin
- Bill of Lading
- Insurance Certificates
- Packing List
- Import and/or Export License
- Consular Invoice
- Letter of Credit and/or Purchase Order
- Ships Cargo Manifest

The container industry's focus remains on the documentation required by U.S. Customs, because this is the information which the security of the U.S. relies on. Customs bases a majority of their security screening on information provided by the bill of lading and cargo manifests. They utilize an Automated Targeting System (ATS) to analyze the data provided and search for anomalies. Customs also aggregates intelligence and threats from agencies such as the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI). Cargo manifests must be transmitted electronically and early enough to meet the government's needs, as a result of requirements set forth by the Trade Act of 2002 (Public Law 107-210) as amended by the Maritime Transportation Security Act of 2002 (Public Law 107-295).

### **Information Filing**

The provisions in the Maritime Transportation Security Act of 2002 establish a program to ensure greater security for United States seaports. As outlined in the Act, for every land, air, or vessel carrier required to make entry or to obtain clearance under the Customs' laws of the United States, the pilot, master, operator, or owner of such carrier (or the authorized agent of such owner or operator) shall electronically provide a cargo manifest 24 hours prior to loading. Cargo manifests must include (Congress 2002):

- The port of arrival or departure (whichever is applicable)
- The flight, voyage, or trip number
- The date of scheduled arrival or date of scheduled departure
- The request for permit to proceed to the destination, if applicable

- The numbers and quantities from the carrier's master air waybill, bills of lading, or ocean bills of lading
- The first port of lading of the cargo
- A description and weight of the cargo or, for a sealed container, the shipper's declared description and weight of the cargo
- The shipper's name and address from all air waybills and bills of lading
- The consignee's name and address from all air waybills and bills of lading
- Notice that actual boarded quantities are not equal to air waybill or bills of lading quantities, except that a carrier is not required by this clause to verify boarded quantities of cargo in sealed containers
- Transfer or transit information for the cargo while it has been under the control of the carrier
- Warehouse or other location of the cargo while it has been under the control of the carrier

The cargo manifest filed by a carrier was never designed to provide all the information that might be relevant to a security analysis, and it is not likely to ever do so, because that would require information beyond the knowledge of the carrier and involve commercially sensitive information that shippers may not want to share with a carrier. Until a new system is developed, cargo manifests will be the interim means to gather relevant information. The public law passed (Public Law 107-295) acknowledges that cargo manifests are not to be perceived as the means to gather any and all information of interest.

### **Information Timing**

Today, cargo manifests are required to follow the U.S. Customs' "24-hour rule". Effective December 2, 2002, Customs regulations have been amended and the rule has been published in the Code of Federal Regulations (CFR) (19 CFR Parts 4, 103, et al.) regarding the 24-hour Advance Manifest Policy. The rule requires all ocean carriers or NVOCCs to submit a complete cargo manifest to U.S. Customs at least 24 hours prior to cargo loading if that vessel is calling a U.S. port directly. The rule extends not only to U.S. imports, but also to cargo transiting U.S. ports and remaining on board the vessel for subsequent discharge at a non-U.S. port. For U.S. cargo moving via Canadian ports, U.S. Customs has begun working closely with their Canadian counterparts. Details of the cargo manifest must be based on actual declaration of cargo by the shipper. The 24-hour period is measured against the scheduled commencement of loading for each non-U.S. port to a vessel destined or transiting a U.S. port. Failure to comply with this rule could result in cargo hold at origin port, significant penalties against the carrier or NVOCC, along with the removal of container for inspection by U.S. Customs and/or the denial of permission to unload vessel cargo and the possibility of returning cargo to the load port (OOCL 2002).

### **Detail and Accuracy**

In modern ocean-borne transportation, the shipper is the party that provides the bill of lading information to the carrier. The carrier essentially transcribes the information into its system and issues a bill of lading on the carrier's form. Consequently, cargo documentation information is actually provided by the shipper. The mandatory information required to meet U.S. Customs directives include (USCBP 2002):

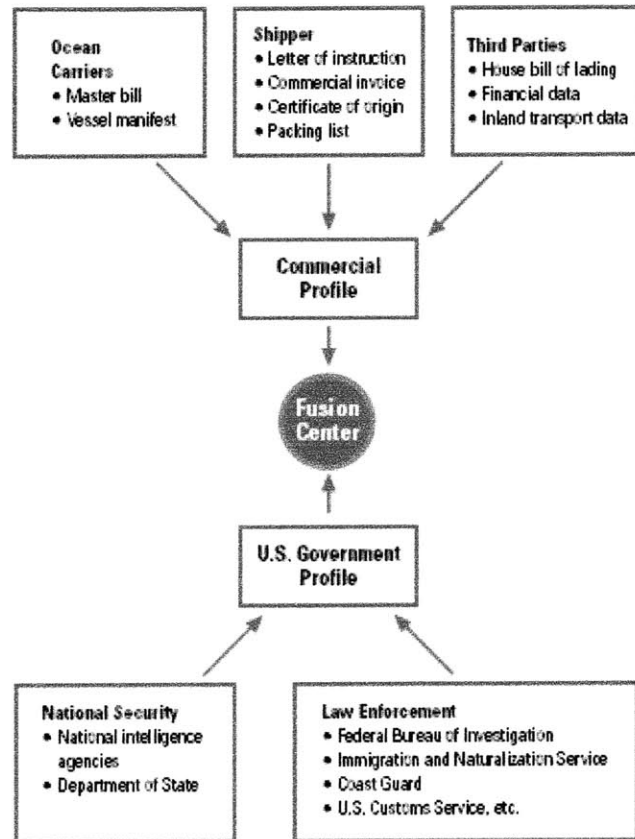


- Shipper and consignee complete name and address
  - Note: Individuals and businesses acting as intermediaries (consolidators, NVOCCs, moving and storage companies, freight forwarders, or brokers) are not recognized by U.S. Customs as the shipper/consignee
- Precise description of the of the commodity with specific weight, piece count, and package type
- Container number and seal number
- Hazardous material code if applicable

#### **Automated Targeting System (ATS)**

The Automated Targeting System (ATS) is an information system designed to assist Customs officers in identifying which containers pose a “high-risk” of containing narcotics or other contraband. The system standardizes the bill of lading, entry, and entry summary data received from the Automated Commercial System (ACS) and creates integrated records called “shipments”. ACS is a comprehensive electronic information system used by Customs to track, control, and process all commercial goods imported into the U.S. These shipments are then evaluated and scored by ATS, through the use of over 300 weighted rules derived from targeting methods used by experienced Customs personnel. The higher the score, the more the shipment warrants attention (USCBP 2003). As previously mentioned, Customs uses the ATS system to screen 100% of all containers before they are loaded aboard a vessel bound for the U.S. As it has refined ATS, ocean container inspection rates have increased, from less than 2% before September 11<sup>th</sup> to a current rate of 5.4%. That means that Customs is now inspecting almost 400,000 ocean

containers per year. The World Shipping Council (WSC) predicts that as Customs further implements its C-TPAT program, and as it refines ATS, it is likely that the inspection rate could grow to 10% (Koch 2004). Figure 4 below shows a basic outline of the information flow ATS is currently utilizing to accumulate available intelligence.



**Figure 4 – Information System Outline (Binnendijk 2002)**

**Summary**

Cargo documentation is a critical aspect of container security. Documentation, which is required for every container shipped globally, can provide vital intelligence to security officials. With the proper information systems at hand, this information can be scanned, searched, and analyzed quickly and in real time.

In order to properly and effectively address this issue, the world must come together and implement a system which is internationally compatible. There are many different technologies currently on the market, and many more under development which will provide this capability. One example is the use of radio frequency identification (RFID) tags. If these tags were used on every container, the container documentation could be stored digitally within the tag, and the container could be tracked end-to-end through the entire supply chain. Anomalies, such as if the container was opened unexpectedly, or it deviated from the expected route of travel, could easily be detected with the proper application of an information system. These physical solutions will be explored in more depth in Chapter 5.

Through information sharing and important relationships between the public and private sectors, such as those being developed within C-TPAT, the suspect or high risk containers can easily be profiled and picked out of a shipment of containers. Then, the field is narrowed, and the chances of catching or detecting a container that could be used for smuggling a WMD, are much greater.

One specific issue that should be addressed is the accuracy of the cargo description. The ocean carrier by necessity must rely on the shipper's declaration to the carrier of the cargo, because the carrier cannot open and verify the contents of sealed containers or crates. Existing Customs' law does not clearly require the shipper of the cargo, who has the necessary cargo information, to provide complete and accurate cargo descriptions for the carrier's cargo manifest. Yet, carriers are subject to penalties for inaccurate information filed for Customs' entry purposes. The law's current penalty provisions

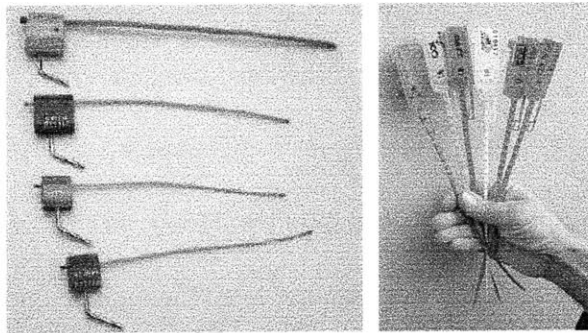
authorize penalties only on the ocean carrier in cases where the cargo description on the manifest is incomplete or inaccurate. This may have made sense in the pre-containerization days when the law was written and when carriers physically handled all the loaded cargo, but it is anachronistic and inappropriate when applied to cargo in sealed containers. With sealed containers, the ocean carrier by necessity must rely on the shipper's declaration to the carrier of the cargo because the carrier does not, and cannot, open and verify the contents of a sealed container.

The container industry and the government must work together to find the critical balance between too much information and not enough. Shippers do not want to completely divulge everything about their shipments due to the sensitivity of this information relative to their competitors within a certain market or industry. The amount of cargo, the carrier utilized, and the timing of shipments can all play critical roles in the dynamics of competitive markets. There are two solutions to this problem. One solution is for Customs and the private sector to settle on a middle ground which will ensure the security of the U.S. The other solution is for Customs to allow the shipper to directly submit the information on their cargo electronically and confidentially to a secure Customs' database.

## CHAPTER 5: PHYSICAL SECURITY

### Background

Container shipping is a highly competitive, low cost, commodity industry. Container shipping companies are constantly looking for ways to minimize costs and shipping rates are highly competitive. This creates an industry with tight budgets and low profit margins. Therefore, companies are very hesitant to spend money on expensive seals or devices to secure their cargo. According to U.S. Coast Guard Licensed 3<sup>rd</sup> Mates, Dalton J. Stupack and Kendall H. Chauvin, most containers carry either a plastic indicator or, on some of the more valuable shipments, a cable seal. They also report that it is not uncommon to see containers aboard ship with no seal at all. These common container security seals are shown below in Figure 5.



**Figure 5 – Common Container Security Seals**

These seals are disposable and inexpensive. They are individually numbered to ensure each seal is unique. However, there are many loop holes and methods to circumvent this type of seal and infiltrate a container. This type of vulnerability could prove to be a costly mistake and it must be addressed by the entire industry.

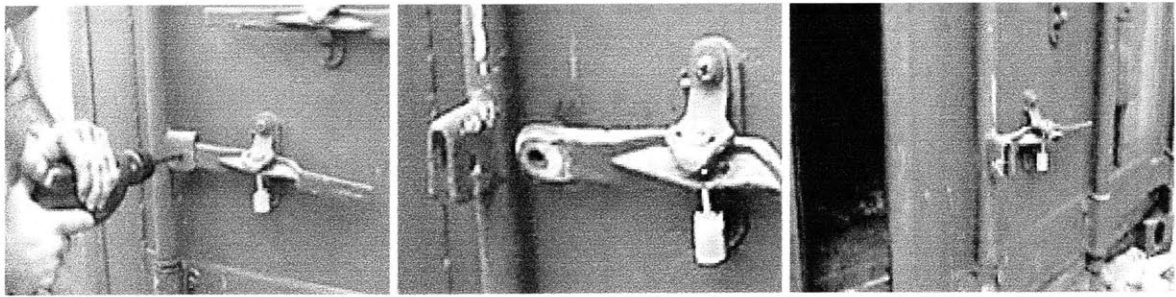
## **Theft**

Prior to September 11<sup>th</sup>, container security was primarily focused on deterring thieves, stowaways, and drug traffickers. The enormity of the problem is hard to overstate. Some estimates put losses due to cargo theft at \$10 billion annually. In southern Florida, police note that many criminals formerly in the drug trade have switched to cargo theft because the financial rewards are so large and the penalties, especially in comparison to narcotics, are slight. The scale of losses from theft illustrates the relative ease with which containers can be infiltrated, and highlights the point that the current measures in place to secure containers are deficient. Consider the different forms of container theft that are about to be presented options which terrorists have should they choose to use a container to smuggle weapons.

One of the most common methods of stealing a container is simply to hijack the truck carrying it. There is the bogus official method, commonly known as the “jump up”, where somebody with a white coat and a clipboard stops the truck just short of the depot that is the destination and redirects the driver somewhere else. There are cases of bogus premises being set up complete with letterhead and logo. These thieves certainly take advantage of the driver’s inability to speak the local language. Another common method is to steal the truck when it is unattended. The thieves often know exactly what their target is, and have teams of scouts in place with cellular telephones. They strike as soon as the driver has gone to have a meal or a shower, either absconding with the truck or stealing the goods out of the container and resealing it.

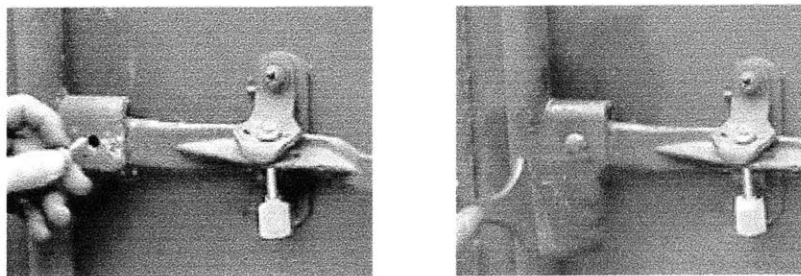
Fraud is also a method used by thieves. A typical trick used by container thieves is to use forged documents to obtain the release of the containers from ports or container yards. Most of the fraud cases have some form of insider help. Staff members have been bribed or intimidated; sometimes it is the importers themselves who arrange the theft to reduce their own costs. Law enforcement officials and security experts often report that a majority of theft is internal, either the work, or result, of information provided by insiders. The fact, that usually only high-value cargo is stolen, indicates that the thieves have knowledge of a container's contents.

Container thefts do not necessarily involve stealing the container itself. A group of criminals that has the time and resources will take a container and cut a hole in the side or the roof of the container to remove some, or all of the contents. The hole is then re-welded and painted over, looking like a bad repair, and the seal, which is designed to show if the container has been tampered with, remains unbroken. Or they remove the rivets holding the doors on, and replace them afterwards. When the theft is discovered at the destination, there is no clue as to when or where the theft occurred. Figure 6 below shows what some thieves believe to be the weakest link in cargo container security, the bolt connecting the handle to the locking bar. In less than two minutes, simply using a common household electric drill, the handle can be disconnected from the locking bar. The result is an open door without the seal ever having been touched.



**Figure 6 – Bolt Removal and Open Door Process**

It is a simple matter to insert a replacement bolt and add a few dabs of touch-up paint as shown in Figure 7. Even the trained eye of a marine surveyor will be hard-pressed to notice the evidence of tampering. The seal is intact, never having been touched. No one will discover the break-in until the container reaches its destination thousands of miles away. By that time, the container has been interchanged between several carriers; thus, by whom and when the loss occurred can never be determined. This uncertainty will lead to the denial of liability by each and every carrier. Denial of insurance coverage is also extremely likely.



**Figure 7 – Bolt Replacement and Touch-up Paint**

Currently, there are a vast number of vulnerabilities and methods available for terrorists to infiltrate a container. The existing technology and equipment used to seal containers is not enough to keep our country safe. Therefore, new technologies must be



implemented into each and every container thus improving the integrity of all shipments entering the United States.

### **Technological Advantages**

The main keys to improving security are visibility and control. The physical seals currently in use have several inherent weaknesses. They cannot determine if the container has been tampered with or not. They cannot provide information on the location of the container if it was hijacked, and they cannot provide information on the route of travel, which the container took should it have been temporarily diverted from its expected route. With this type of visibility and information, a majority of the current problems and vulnerabilities would be dramatically reduced.

Better visibility can be achieved through implementing two systems:

- Information systems that manage, manipulate, or display visibility data
- Event-driven tools that convert physical activities and conditions into data entries for the software systems, also known as freight identification technologies

Freight identification technologies provide vast amounts of information on thousands of shipments per day. Therefore, the trend is moving towards Automatic Dependent Surveillance (ADS) of these shipments and the information which is provided by these technologies. ADS is a term used in air and vessel traffic control for on-board equipment that automatically determines location and other relevant information without intervention from crew or network managers. The most critical element of ADS, with regards to container shipping, is the fully automated byproducts of the operation. The data recording and identification methods are triggered by the movement and traffic management

processes. Condition changes will be detected and stimulate reports due to sensor changes such as an opened door or measurements that move beyond a threshold such as temperature changes. These technologies are completely automated and eliminate human labor from these monitoring demands.

### **Electronic Cargo Seals**

Electronic cargo seals (e-seals) are a subset of sensor technology and are receiving serious consideration from DOT, U.S. Customs, and other government agencies. E-seals are much more robust and have much greater security capabilities than their simple, low cost, mechanical counterparts. E-seals tend to combine physical seals with RFID components. Most of the electronics include passive or active type RFID technologies.

Passive seals are short range, low cost, and disposable. They have no inherent electric power such as a battery. The RFID reader or interrogator provides energy when it illuminates or scans the seal. The passive seal uses the absorbed energy to reflect its information back to the reader. The lack of on-board power limits the functionality. For example, since passive seals cannot detect and record tampering at the time of the event, they simply report whether they are intact or not when interrogated by a reader.

Active seals are more sophisticated, have higher initial costs, and – until prices drop significantly – demand reuse. Active seals carry batteries and the power permits longer range and greater functionality. To extend the previous example, they can detect tampering when it occurs and add it to a time log of events. If equipped or interfaced with GPS, an active seal can also log the location. Further, some seals can provide live “mayday” tampering reports as the events happen, mostly within specially equipped terminals.

Because of their low unit cost and operational simplicity, passive seals were generally the preferred solution for “pre-September 11” security requirements aimed against theft. The greater the functionality of active seals enhances their appeal for “post-September 11” security against terrorist tampering (Wolfe 2002).

Progress is being made, but there are still several hurdles which stand in the way of wide use of e-seals:

- International standards. The International Standards Organization's (ISO) Technical Committee 104 is close to a decision on a multi-protocol standard that provides for both passive and active seals.
- Global frequencies. Although several initiatives are currently pursuing this issue, currently there are no global frequencies and technical specifications for e-seals or other RFID logistics applications. These specifications would need to address the topics of power levels and duty cycles which can be globally compatible.
- Operating practices. Reusable seals pose an operational challenge for shippers and carriers. However, if that challenge is mastered, then reusable seals also offer an opportunity to lower the per-use cost of high security seals. Two points may mitigate the operational challenges. First, a significant portion of commercial containers operate in repetitive service that is more suited to recycling seals. Second, if empty container movements were sealed for security reasons, that should simplify the recycling process.
- Field experience. E-seals are relatively new to the market and in limited use. It makes sense to conduct a vigorous pilot and demonstration program to accelerate the processes of accumulating field experience, fine-tuning products, and developing customer confidence – all important to support regulatory requirements for e-seals (Wolfe 2002).

### **Security Sensors**

Shippers, carriers, and supporting firms have a history of using sensors to monitor the conditions of cargo, to support safe and efficient operations, and to enhance security, usually against theft.

The best example of monitoring cargo conditions is the temperature of refrigerated products. Some devices are self-contained recorders that move with the shipment and collect temperatures inside the container through points in time throughout the entire shipment. This data is used for quality assurance and assigning liability. Similar devices are used by companies shipping hazardous materials in order to monitor tank pressure and vapor leakage.

Intrusion detection devices, prior to September of 2001, included not only e-seals but mechanical, light-sensitive, and infrared motion detectors as well. Break-wire grids can detect forcible entry through ceilings, sidewalls, and doors. USCBP has a long term interest in Non-Intrusive Inspection (NII) devices and technologies. These include large equipment to scan trailers, containers, and railcars with x-rays and gamma rays, such as the Vehicle and Cargo Inspection System (VACIS). Inspections, including NII, will be explored in greater detail in the next chapter.

### **Wide Area Communication and Tracking**

Wide area communication is an ideal platform on which to integrate condition sensors, transaction confirmation tools, and geo-location information. Dramatic improvements in components, integration, and costs are just now coming to fruition. These dynamic technologies will change today's definition of both good business practices and security. Satellite-based systems are preferable to cellular for coverage areas and potential global applicability. Cellular-based is less expensive and more suitable for domestic applications.

Sensors and transaction confirmation tools are extremely flexible and able to meet a broad range user needs. Examples include WMD sensors, RFID transponders for precision gate arrival confirmations, e-seal integration, and asset management sensors, such as empty / partial / full indicators.

One important consideration for wide area platforms is the electrical power needed to drive the sensors, capabilities, and communications of the platform. Power is not an issue for conveyances that generate their own electricity. However, it is a major problem

for devices with no access to external electricity, as would be the case for non-refrigerated freight containers. Battery failure troubled the U.S. Army's early experiments with RFID tags on containers. In-the-field, battery replacement was found to be both cumbersome and expensive.

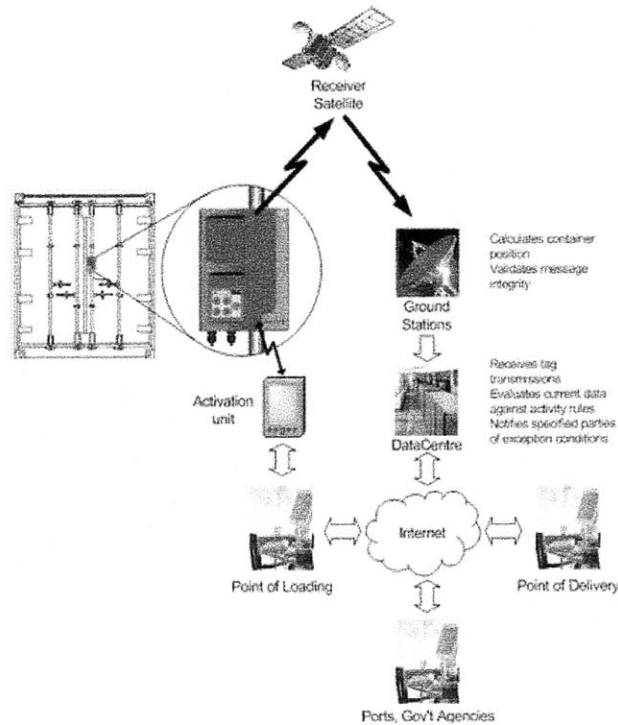
Power is one of the major limiting factors for the implementation of this technology. Engineering of these devices should be directed to a low level of power consumption. This has already been achieved in some GPS units available off-the-shelf.

### **Information Systems**

Enhancing the security of the container industry requires information systems that can aggregate, sort, and analyze all the data and information, which will be provided by these technologies. The information systems must have the capabilities to register the alerts generated by the equipment, and analyze the cargo information in order to detect anomalies. For instance, the information system should have the capability to pick out an inconsistency, such as a container of cotton balls weighing 30,000 lbs. Capable information systems are the most crucial element to an effective risk management security solution.

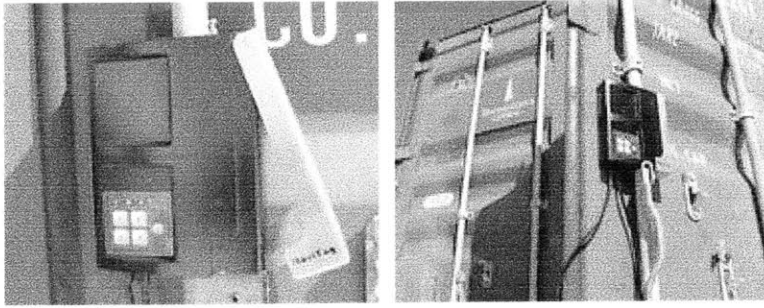
### **Technology Available**

One example of technology that is currently being developed, which encompasses the recommendations made in this thesis, is the NaviTag unit produced by NaviTag Technologies. The NaviTag CTU utilizes a low power, satellite transmitter that allows it to communicate from anywhere in the world. The satellite communication network is shown in Figure 8.



**Figure 8 – Example Satellite Communication Network**

This transmitter, in conjunction with door and light sensors, provides the capability to send positional and door open conditions on a regular basis throughout the container's journey to its destination. The CTU provides this functionality in a self-contained unit at a size and price point not previously available. The CTU is about the size of a paperback novel, universally fits on any ocean container, and is light in weight to facilitate return shipment (see Figure 9). It attaches to the locking bars on the exterior of the container door and is securely locked in place for the duration of the voyage. It is easily detached at destination by entering the correct unlock code into the electronic keypad.



**Figure 9 – NaviTag in the Field**

Since the NaviTag CTU is, by design, a removable device, each cargo tracking session is required to be registered. The NaviTag Technologies solution is to initiate each cargo tracking session by associating a NaviTag with the cargo's container number and its ultimate destination. These initialization values are input into a registered activation unit and transferred to the CTU via an authenticated infrared link. In addition, this activation unit maintains a bi-directional connection with NaviTag Technologies, providing a channel for future enhancements and upgrades.

Once the CTU has been activated, it transmits positional and status information to the DataCentre at an average of every one and a half hours. The DataCentre receives and validates the transmissions, runs rules and evaluations against these transmissions, and stores the data for future evaluation. If any voyage activities warrant notification, the DataCentre will generate messages to the appropriate parties. The rules, messages, and notification parties are customer specific and can be modified easily to accommodate individual company and voyage requirements.

### **Summary**

The security of the freight container, at present, leaves much to be desired. This chapter outlined a physical solution to improving the security of containers entering the

United States. When implementing and relying on such technology to ensure that the shipment is secure, Customs must now step up procedures to validate the security of the shipper's loading practices.

The technology is available. International harmonization and testing of this technology must be achieved in order for the implementation of this solution to become an effective means of fighting terrorism. This technology not only provides substantial improvements in security and visibility, but it has the potential to vastly improving supply chain management. The potential for this type technology, which can improve both security and save companies money in their logistics and inventory management, will be investigated in depth in Chapter 7.



## CHAPTER 6: INSPECTIONS

### Background

The combination and integration of cargo certification, documentation, and the physical security described in the previous two chapters is essentially an effective risk management approach to container security. The last step to implementing a successful risk management program is inspecting all of the suspicious cargo.

At its heart, risk management presumes that there is a credible means to (1) target and safely examine and isolate containers that pose a potential threat, and (2) identify legitimate cargo that can be facilitated without subjecting it to an examination. The alternative to risk management is to conduct random inspections or to subject every cargo container to the same inspection regime. Risk management is the better of these two approaches for both economic and security reasons. The economic rationale is straight forward. Enforcement resources will always be finite and delays to legitimate commerce generate real costs.

Less obvious is the security rationale for risk management. There is some deterrent value to conducting periodic random inspections. However, since over 90% of shipments are perfectly legitimate and belong to several hundred large importers, relying on random inspections translates into spending the bulk of time and energy on examining those containers by the most frequent users of containerized cargo who are most likely to be perfectly clean.

“Examining 100% of all containers is not only wasteful, but it violates an age-old axiom in the security field that if ‘you have to look at everything, you will see nothing’. Skilled inspectors look for anomalies and invest their finite time and attention on that which arouses their concern. This is because they know that capable criminals and terrorists often try to blend into the normal flow of commerce, but they invariably get some things wrong because they are not real market actors. But, an aggressive inspection regime that introduces substantial delays and causes serious disruption to the commercial environment can actually undermine an enforcement officer’s means to conduct anomaly detection. Accordingly, allowing low risk cargo to move as efficiently as possible through the intermodal transportation system has the salutary security effect of creating a more coherent backdrop against which aberrant behavior can be more readily identified (Flynn 2003).”

Traditionally, the U.S. Customs relied on physical inspection of cargo as the primary method to determine whether what was being imported into the United States matched what was on the bill of lading or other documentation. In part, because compliance rates were fairly high, physical inspection rates fell to as low as 2% (Bryant 2003). This means that 98% of the cargo being shipped into the United States was not examined by the federal government, which placed heavy reliance on the good faith of the shippers and the accuracy of the documentation. That worked adequately when the only risk was commercial underreporting and the occasional smuggler. However, the terrorist attacks dramatically changed the risk factors and now Customs cannot simply rely on the good faith of shippers.

Today, Customs uses the ATS system to screen 100% of all containers before they are loaded aboard a vessel bound for the U.S. As it has refined ATS, ocean container inspection rates have increased, from less than 2% before September 11<sup>th</sup> to nearly 6% in 2003 (Flynn 2003). That means that Customs is now inspecting almost 400,000 ocean containers per year. The inspection rate is expected to continue to increase this year.

As noted, currently, approximately 6% of all inbound ocean containers are physically searched or inspected using non-intrusive technology. As Customs further implements the C-TPAT program, and refines ATS, it is likely that the inspection rate will increase further. Some projections have Customs' inspection rates growing up to 10%. However, the numerical objective should not be the goal. The goal should be to inspect 100% of all containers that ATS says warrant inspection, plus some random process designed to monitor and verify the selectivity techniques being used.

Increasingly, physical inspection by Customs officials is a last resort. Physical inspection of one container might involve two inspectors and last a full day. Therefore, technological inspections are being conducted with increasing frequency. Also known as non-intrusive inspections (NII), these technological inspections are the solution to greater detection and visibility while decreasing man power and time. These detection devices are also capable of identifying nuclear weapons, radiological materials, chemical and biological agents, and conventional explosives. Employing these devices at ports of embarkation, where containers are loaded onto vessels, is an important element in enhancing security. Technologies must be suitable for use on closed containers in a port environment where speed, ease of use, and low false alarm rates are critical.

## **Non-Intrusive Inspection (NII) Technology**

NII Technologies can be grouped into two general categories: active systems or passive systems. Active systems are made up of technology that stimulates the object under inspection in some fashion, and the resulting effect is subsequently sensed by detectors. Passive systems are made up of technology that detects some unstimulated emanation coming from the cargo. The following definitions were created by the Sandia National Laboratories report “Survey of Commercially Available Explosives Detection Technologies and Equipment” created for the National Institute of Justice, September 1998.

### Active Systems

- *Acoustic*: An ultrasonic transducer is put into contact with the container and scanned. A sensor then detects the resulting reflection from objects inside and forms an image of them. The technology is useful only in liquid (tanker truck) environments.
- *Gamma Ray*: The use of an active (radioactive) element (usually Cesium<sup>137</sup> or Cobalt<sup>60</sup>) to produce gamma rays aimed at the object under inspection. The rays interact with the object, are detected and are displayed as an image. Gamma ray systems are transmission only. Cs<sup>137</sup> emits radiation at 662 keV, and Co<sup>60</sup> emits both 1.2 MeV and 1.3 MeV radiation.
- *Pulsed Fast Neutron Analysis (PFNA)*: Pulsed neutrons are created and directed at the object under inspection. The neutrons interact with the elemental constituents of the object and create gamma rays with energies characteristic of its elemental composition. From the energy and time of arrival of the gamma arrays in detectors, an elemental

image of the object is created, which can indicate the presence of threat material containing defined concentrations of these elements.

- *Thermal Neutron Activation:* Thermal neutrons are used to interrogate the object under inspection. Sophisticated sensors detect the energy of the gamma ray photon emitted when the thermal neutron is absorbed by material within the object. Because the energy of the photon is highly specific, the detection of photons from nitrogen, for example, may be related to the presence of explosives.
- *X-ray:* The use of a source and appropriate beam forming to generate x-rays aimed at the object under inspection. The x-rays interact with the object, are detected, and displayed as an image. X-ray energies used ranged from a low of 120 keV to a high of 9 MeV, with penetration of the object dependent on the energy used. Systems designed for cargo inspection are normally sized at 320 keV minimum.
  - *Standard Transmission Systems:* The transmission x-ray is directed through the cargo to a detector and presents one “shadowgram” image to the operator that overlays all items in the beam path. Transmission systems operate at all energy levels without restriction.
  - *Dual Energy Transmission Systems:* Two different x-ray energy spectra are used to interrogate an object, and the difference between the outputs of the two is used to highlight various materials. This technique is generally ineffective for large cargoes, because the low energy component does not penetrate through the large mass of material.

- *Dual View Transmission Systems:* Two (usually orthogonal) views of the object, each similar to the images produced by standard transmission x-ray, are created and displayed. The technique is not limited in energy level.
- *Backscatter Systems:* Two or more views of the object are created and displayed: One standard transmission image and at least one image created using Compton Backscatter. The Compton Backscatter detectors are placed on the same side of the object as the illuminating source. Backscatter images highlight items in the object that contain low atomic number (low  $Z$ ) elements, since these items scatter more and create a brighter image than higher  $Z$  materials. Backscatter is useful at energies up to 500 keV, but can be paired with higher energy transmission imaging to enhance operator interpretation.
- *Computed Tomography Systems:* “Slices” of the object are produced by taking several views of the object from different angles. These slices can then be re-assembled to produce a 3-D view. (Although described here for the sake of completeness, this technology is not appropriate for large cargo inspection due to the physical size of a container.)

### Passive Systems

- *Radiation Detection:* A detector measures the ionizing radiation (gamma rays, alpha rays, x-rays, etc.) or other characteristic radiation such as neutrons naturally emitted from a radioactive substance. Typically, the indication is an audible signal or a reading

on a meter. This type of system could be used to detect the presence of a nuclear device or other radiological threat.

- *Canine Use:* Because of their unusually sensitive sense of smell, dogs can be trained to alert their handlers to the presence of explosives and other threat objects. The dogs must be trained for specific materials, and usually have to be rested periodically to be effective.
- *Vapor Detection/Trace Detection:* A “sniffer” type sensor collects air samples emanating from the container, and then analyzes the sample using a variety of spectrographic methods. Alternatively, a physical “wipe” collects particulate matter from the surface of the container, and this wipe is then placed in a device and analyzed as above. The results are used to determine the molecular nature of the material within the container.

Table 5 contains a summary of key characteristics by technology. Technologies have been grouped to keep similar characteristics together.

**Table 5 – Technology Characteristics (Sheridan 2002)**

	Mat'l Discr.	Mat'l ID	Installation	Integration and Info. Mgt.	Procurement Method	Service	Cost
Active Systems							
X-ray							
Standard Transmission	No	No	Mobile, fixed or relocatable sites require local infrastructure of power, road access, personnel facilities and attention to radiation safety	Systems are computer based, and normally employ commercial operating systems. Data is collected and stored digitally. Data transfer is via standard computer media.	Competitive bid process, which usually includes a warranty and service provision	Required on a regular basis, and performed by trained personnel	\$\$\$\$
Dual Energy Transmission	Not effective for dense cargos	No					N/A
Dual View Transmission	No	No					\$\$\$\$
Backscatter with Transmission	Yes	No					\$\$\$\$
Gamma-ray	No	No					\$\$\$
Pulsed Fast Neutron Analysis (PFNA)	Yes	Yes					\$\$\$\$
Thermal Neutron Activation (TNA)	Yes	Yes	\$\$\$				
Acoustic	No	No	Portable/desktop equipment, can be operated by battery or wallplug power				\$\$
Passive Systems							
Vapor/Trace Detection	Yes	Yes					\$
Radiation Detection	No	Limited to presence of radioactive material					\$
Canine Use	Limited to presence of material for which animal is trained	Yes	Requires care, feeding and shelter, together with trained handlers	Stand alone	Competitive bid process for animals, training, and services. Difficult to warranty	Food, training, shelter	\$

Cost Key: \$: ≤ \$50K; \$\$: ≤ \$100K; \$\$\$: ≤ \$1M; \$\$\$\$: ≤ \$5M; \$\$\$\$\$: ≥ \$10M



Table 6 shows how the various technologies address security functions.

**Table 6 – Technology Functionality Matrix (Sheridan 2002)**

	Time for Inspection	Indicates Potential Presence of Threat	Provides Material Discrimination	Identifies Specific Threat	Provides Electronic Record	Integrates with Other Technologies
<u>Active Systems</u>						
<b>Acoustic</b>	2-5 minutes/object	Yes, in liquids	No	No	Yes	Yes
<b>Gamma Ray</b>		Yes	No	No	Yes	Yes
<b>Pulsed Fast Neutron Analysis (PFNA)</b>	90+ minutes/object	Yes	Yes	Yes	Yes	Yes
<b>Thermal Neutron Activation (TNA)</b>		Yes	Yes	Yes	Yes	Yes
<b>X-ray:</b>	2-5 minutes/object					
<b>Standard Transmission</b>		Yes	No	No	Yes	Yes
<b>Dual Energy Transmission</b>		N/A	Not in high density cargos	N/A	Yes	Yes
<b>Dual View Transmission</b>		Yes	No	No	Yes	Yes
<b>Backscatter with Transmission</b>		Yes	Yes	No	Yes	Yes
<u>Passive Systems</u>	0.5-1 minute/object					
<b>Canine Use</b>		Yes	Yes	Yes	No	No
<b>Radiation Detection</b>		Yes	Yes	No	No	Yes
<b>Trace Detection</b>		Yes	Yes	Yes	Yes	Yes
<b>Vapor Detection</b>		Yes	Yes	Yes	Yes	Yes

In general, all of these technologies can be applied to scan containers being transported by any mode. They are typically built to inspect the cargo one container at a time. NII systems help mitigate the risk of a terrorist smuggling a WMD into the U.S. inside a container for several reasons. Radiation detection quickly identifies potential danger from bombs containing radioactive material if unshielded. Containers with the potential of a chemical threat may be identified by a combination of imaging and trace detection if chemicals are unsealed. NII systems provide quick processing times with minimal disruption of flow especially when used in tandem with an ATS. These systems also reduce manpower and therefore operating costs. The presence itself will act as a deterrent to hostile or illegal actions. Finally, the personnel performing the inspections are not subject or exposed to a potentially lethal threat within the container. Radiation detection pagers, x-ray inspection systems, and gamma-ray inspection systems will be explored in more detail since these are currently, and by a large margin, the most common NII systems being put into service all around the world.

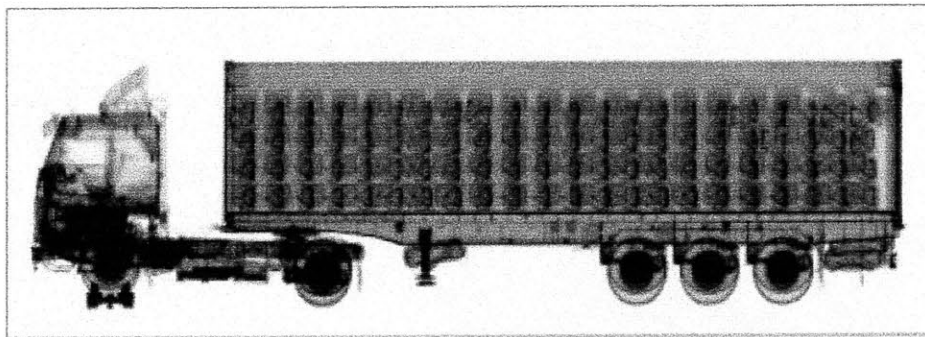
### **Radiation Detection Pagers**

Radiation detection pagers are small, self contained gamma-ray radiation detectors that alert its carrier to the proximity of radioactive materials. Such devices were specifically developed to be used by government agencies and emergency responders and are approximately the size of common message communication pagers. Radiation pagers can be hundreds of times more sensitive than commercially available Geiger-Muller tube type detectors which are of similar size. As an example of the international usefulness of

these pagers, on March 21, 2000, a radiation pager detected radioactive material in a shipment that was transiting Uzbekistan in route to Pakistan (Albright 2001).

### **X-Ray Inspection Systems**

X-ray based inspection systems are the most common form of NII technology in use today. X-rays detect differences in material densities in order to produce an image of the vehicle or container contents. Contraband detection actually occurs by the system operator who visually, sometimes with the help of sophisticated software, inspects the x-ray images for anomalies. A sample x-ray image of a 40-foot fully loaded container with television sets is show below in Figure 10.



**Figure 10 – X-ray image of a fully loaded, 40-foot container (Lecoindre 2002)**

When cargo and contraband are of similar densities, contraband detection is very difficult. For example, “the density of a plantain appears exactly the same as that of cocaine molded and painted to look like a plantain when both are put through an x-ray” (Peters 2001). The density differences are projected across the entire width of the container; if a container is very cluttered, the detection of contraband may be very difficult as the x-ray image will also be cluttered and visually complex. Additionally, due to the projection methods, contraband could be hidden in the shadow of a very dense piece of cargo. However, the use of multiple x-ray beams can erase most of the shadow effects. As

an example, the above image is of a tractor-trailer filled with television sets; with such a complex image, it is clear that the detection of contraband may be very difficult. Due to the nature of x-ray methods, specific materials cannot be identified; more advanced technologies like gamma-ray systems can detect specific materials like drugs and explosives.

X-ray systems generally take a few minutes to scan a standard 40-foot container while some more advanced systems can take only a few seconds. However, total inspection cycle times may range from seven to fifteen minutes or longer due to image analysis (Bowser 2002). This could result in scanning less than 100 containers per day.

### **Gamma-Ray Inspection Systems**

Gamma-ray inspection systems are an alternative to standard x-ray inspection systems. These systems directly use gamma-rays or use pulsed fast neutrons to generate gamma-rays to produce images of the container's contents, 3-D mappings of content location, as well as other important information. For example, some systems can also determine certain types of material inside the container based on atomic characteristics; a few of these detectable materials are carbon, nitrogen, oxygen, silicon, chlorine, aluminum, and iron (Brown 2002).

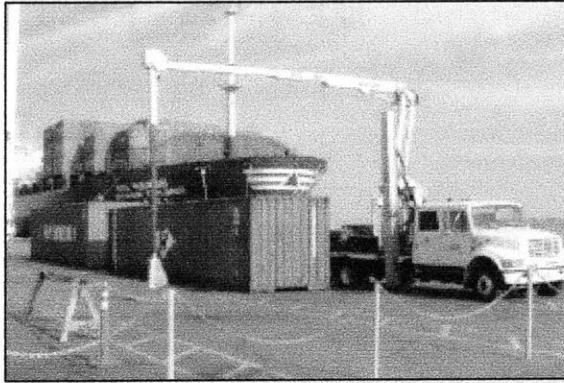
Claiming many benefits over x-ray technology, these gamma-ray systems may be a key step towards an efficient NII process. Gamma-ray systems can scan standard 40-foot containers in a few seconds and generate a total inspection time of less than a minute. The average inspection throughput of a gamma-ray system is more than ten times faster than

the quickest x-ray system. In a trial at the Port of Miami in 1998, a single gamma-ray inspection unit resulted in the inspection of over 1,300 TEUs in a single shift (Snell 2002).

Gamma-ray systems can be produced as fixed-site, semi-fixed-site, or mobile units. The semi-fixed-site units can be moved and set up in one to two days while the mobile units can be driven to any spatially accommodating location in the port and can be made operational by three people in approximately ten to fifteen minutes (McBee 2002). Fixed-site systems may be of a pass through inspection type unit. Current vehicle pass through speeds are approximately four to five miles per hour with future plans of more than ten miles per hour. The systems can scan almost all types of cargo handled in the port including standard containers, bulk cargo containers, truck trailers, and rail cars. Fixed-site and mobile unit gamma-ray systems are pictured below in Figures 11 and 12.



**Figure 11 – Fixed-site, rail-mounted unit (Snell 2002)**



**Figure 12 – Mobile unit (McBee 2002)**

Gamma-ray systems can cost from 3-20 times less than x-ray systems in terms of initial capital investment and 4-5 times less in terms of installation costs. When considering other benefits, gamma-ray systems can yield a cost per inspection that is 50 times less than that of conventional x-ray systems (Snell 2002).

Mobile gamma-ray inspection units were heavily utilized at the Port of Vancouver, Canada in 1999 and 2000 and were responsible for the discovery of \$700,000 worth of stolen automobiles ready for illegal exportation. In the previously mentioned 1998 trial at the Port of Miami, during the first 90-days of use, gamma-ray inspection units were responsible for the recovery of six stolen vehicles worth over \$200,000 (McBee 2002).

### **Summary**

All technologies discussed have some measure of effectiveness in uncovering WMDs concealed in containers that travel across the world. No one technology possesses all the characteristics that would make it the ideal system. The most optimal solution is to have a series of systems, each with its own strengths, that permits an inspector to make the most informed decision as to the probability of a particular container housing a lethal threat. For example, a radiation detector coupled with a gamma-ray inspection system and

a vapor/trace detection system provides an abundance of information at a nominal cost.

Such an approach is feasible and the technology to implement it exists today.

## CHAPTER 7: ASSOCIATED COSTS

### Background

There are three categories in which the impacts of terrorism and security countermeasures can be divided:

- Primary Impacts
- Secondary Impacts
- Indirect Secondary Impacts

Primary impacts result from successful terrorist incidents. The focus is on actual damage, casualties, and disruption. Direct secondary impacts encompass the effects of the rescue and recovery effort. The focus in this second type of impact is on clearing damage, mobilizing support resources, and mitigating congestion.

Indirect secondary impacts result from countermeasures to deter terrorism and altered behavior due to the attack, not the actual attack itself. The initiator of the impact is not solely public policy; it may be private companies or other for-profit and volunteer organizations as well. The implications of indirect secondary impacts can be profound due to their geographic breadth, functional scope, and potential persistence over time. There are few exceptions to the rule that indirect secondary impacts are likely over time to outweigh primary and direct secondary impacts.

Indirect secondary impacts of security countermeasures are fundamentally economic. They can erode productivity by increasing the cost of providing private and public services and by disrupting efficient business processes. Impacts can also be



positive, such as eliminating network bottlenecks in mid-Atlantic rail service or improving intransit visibility. Some indirect secondary impacts are rather straightforward and well commented upon. Other impacts are more subtle, or less obvious, or less the subject of public discussion (Wolfe 2001).

There is no comprehensive information about added costs of security measures, only suggestive discussions, anecdotes, and occasional nuggets of data. For example, Robert Delaney, a respected observer of logistics trends, estimated that trucking and airfreight carriers would incur \$2 billion in added security costs. If Delaney is correct, then his aggregate cost estimates should be considered relative to carrier profits and profit margins. That comparison makes security costs appear more daunting because margins will not sustain large new investments in security.

Insurance is an important component of increased security costs. Rates, already rising for most freight-related coverages, accelerated after September 11. No mode was unscathed. Better security practices should yield lower future premiums for theft coverage, but they are unlikely to lower terrorism or war risk premiums. Rates are a useful measure, but Total Cost of Risk is a better metric: “the sum of a company’s outlays for insurance, retained losses, and risk management administration.” Insurers raised deductibles, are refusing coverage in more cases, and some are withdrawing from cargo business lines. The Total Cost of Risk is rising faster than rates. Some shippers and carriers will be left with much greater risk exposure, and major losses could put corporate survival at risk (Wolfe 2001).

This chapter is to provide insight into the major costs associated with terrorism, impacts, and security measures recommended for the container industry. There are four groups of costs that should be addressed when analyzing container security:

1. Direct costs of implementing suggested technology
2. Incurred cost due to indirect secondary impact of increased inspections
3. Revenue lost due to smuggling and theft
4. Potential cost savings due to enhanced supply chain efficiency

The costs of implementing the overall security solution proposed in this thesis should be shared by both public and private sectors. The Department of Homeland Security has allocated additional resources since September 11<sup>th</sup> aimed at improving the areas of documentation and inspections. Funding has been directed towards improving the Automated Targeting System, installing Non-Intrusive Inspection technology into container terminals, and allocating Customs officials dedicated to inspecting cargo.

The private sector can dramatically improve supply chain efficiency, information, and control by installing the security and tracking technology suggested in Chapter 5. The potential for cost savings realized by companies who implement such technology will be established in this chapter. The net benefit of implementing such technology is extremely contingent upon the value of goods being shipped. Therefore, on average, the net benefit realized by shippers will range from \$300 to \$800 per container. The benefits that are difficult to capture numerically such as enhanced customer service and the value of human lives saved are not included in the net benefit presented. These benefits go above and beyond cost savings and should be additional motivation for the private sector to step up container security. Due to this win-win situation, private industry should help bear the burden of enhancing the physical security of the containers.

### **Direct Costs of Implementing Technology**

The direct costs of implementing the suggested technology can be broken down into three primary areas:

- The costs of the actual hardware – RFID tags, readers, and signposts

- Service costs associated with planning, designing, configuring, and installing hardware
- Service costs associated with maintaining a secure, accessible, and timely network

Infrastructure costs include the network equipment installed permanently at ports and terminals, RFID seals applied to each container, and handheld readers at customer specific locations. Implementation costs include personnel and travel expenses required to assess, design, implement, test, and analyze the system. Operation costs include the maintenance of the existing infrastructure and the costs of operating the information database and interface. A service provider will be required to make a large, upfront investment to build up the system before any revenue has been realized. Table 7 below are critical cost assumptions to implement an RFID tracking network solely between Thailand and Seattle. However, in order to make the service attractive to a large number of shippers utilizing, the service providers will have to implement an extremely robust system. RFID readers and signposts will have to be installed at multiple terminals and ports. Within each terminal at the ports, readers will have to be installed in a way to ensure that both a container's arrival and departure are recorded. Additionally, the solution requires the use of handheld readers at the origination and delivery points.

**Table 7 – Costs of Implementing a Tracking Network between Thailand and Seattle (APEC 2003)**

Expense	Cost	Frequency
Infrastructure	\$ 436,389	One Time
Implementation	\$ 3,433,046	One Time
Variable	\$82	Per Container
Operating	\$ 100,000	Per Year

A cost-benefit analysis was performed by Bearing Point for the Asia Pacific Economic Cooperation's Secure Trade in the APEC Region - Bangkok Laem Chabang Efficient and Secure Trade (APEC's STAR-BEST) Project. The project determined the costs and benefits of implementing an RFID network between Laem Chabang, Taiwan and Seattle, Washington. The project concluded:

The financial viability of a full-scale implementation of the solution across the Laem Chabang to Seattle tradelane is heavily dependent on three key factors: volume, revenue per container, and implementation time. To gain profitability, the service provider must cover both variable and fixed costs. At a minimum, the revenue per container must meet the variable costs. In this case, the RFID tag and bolt cost of approximately \$85 serves as that bottom range. As the revenue per container increases, the number of containers that must be moved through the system decreases. Given a likely price point of approximately \$220 per container and the cost assumptions given in Table 7, the service provider would need to deploy a solution to support approximately 8,000 containers annually to realize positive returns over five years. (APEC 2003)

### **Indirect Secondary Impact: Increased Inspections**

U.S. Customs currently inspects a small percentage of containers that arrive at U.S. ports. While the risk that any one container will be selected for inspection is small, the costs incurred by the importer in such a case can be high. The delay in getting the container from the port to the distribution center (DC) adds to carrying costs. Random inspections add variability to expected transit times and forces the importer to increase safety stock levels. Customs guarantees that inspections will be reduced for containers originating from companies in compliance with C-TPAT. It can also be assumed that containers utilizing the RFID solution would receive even more favorable inspection rates. A substantial drop in the probability of inspection could lead to substantial cost savings.

Safety stock, the amount of inventory that must be kept on hand to ensure a target service level, is highly dependent on transit time magnitude and variance. Reducing the time it takes goods to be delivered to DCs, and the variability in that time, reduces the amount of inventory a company must maintain on hand to guarantee service.

The network solution of implementing RFID and readers on containers has the capability of reducing both time and variability. Variability would also drop as more containers move straight from the terminal to the DC and as logistics personnel are empowered to optimize decisions based on real time information. RFID allows for greater supply chain visibility and confidence as the physical events of container flows are closely connected to the data flows. The system provides exceptional management and decision making capabilities to the shippers as problems arise. This leads to further potential savings. The system will identify inefficiencies in the supply chain such as unnecessary delays at ports, multiple transshipments, and misdirected containers. The shipper will also be alerted immediately of such inefficiencies and can act to correct the problems.

The following economic model was developed by Hau L. Lee and Seungjin Whang at the Graduate School of Business, Stanford University. The model captures the savings due to inspections and safety stock as previously described. The lessons of successful quality improvement programs were applied to develop the model. The central theme of the quality movement – that higher quality can be attained at lower cost by proper management and operation design – is applied to supply chain security (Lee 2003).

Let  $p$  be the inspection rate of containers arriving at a destination port. Therefore,  $p$  can be interpreted as the probability that a container load will be inspected by Customs. Given the heightened concerns of terrorism and WMD, and the use of ATS, U.S. Customs has increased  $p$

from its former level. The immediate effect of this increase is that the direct cost of inspection will increase, and it is expected that this cost will be passed onto shippers and carriers. Besides the direct inspection cost, additional inspections have led to congestion at the destination ports, due to limited inspection resources. A simple queuing model can be used to quantify the additional waiting time for the increased inspection. The effect of increased inspection to overall transit time of shipments is therefore: (1) added variability due to the fact that more will now go through the inspection process; (2) added mean lead time with a greater fraction of shipments going through inspection process; (3) additional variability of transit lead time due to the variability of waiting time at the port as the shipment goes through inspection.

The overall lead time, given by the sum of the transit (transportation) lead time and the inspection dwell time (which would be zero if a shipment does not have to go through inspection, but a random variable equal to the total waiting time of the queuing system at the inspection point), will ultimately affect both the pipeline inventory (using Little's Formula) as well as the required safety stock at a distribution center in the destination country. Suppose that the transit lead time is independent of the inspection dwell time (Lee 2003). Let:

$x$  = transit lead time in days, a random variable

$y$  = inspection dwell time in days, a random variable

$T$  = total lead time in days

$$E(T) = E(x) + pE(y)$$

$$\text{Var}(T) = \text{Var}(x) + p\text{Var}(y) + p(1-p)[E(y)]^2$$

Note that  $E(y)$  and  $\text{Var}(y)$  are given by the queuing model that describes the inspection process.

An approach to container security using RFID and other technologies already in use applied to container security and tracking will have several impacts. First, electronic submission of the bill of lading will be made possible and comply with Customs' 24 hour rule. This will reduce the time that the manufacturer and the shipping lines have to spend delivering the bill of lading to Customs. The result is savings in labor costs and some

reduction in the in-transit lead time, which in itself has implications for in-transit inventory and safety stock at the DC. Several shipping companies today have already implemented these automated processes.

Second, with the containers equipped with the electronic seals and the processes for source loading and in-transit shipment both tightly monitored, with the full compliance of the 24 hour rule, and with a C-TPAT membership, U.S. Customs guarantees they will not apply the same intensity of inspection.

Third, with increased visibility throughout the supply chain, and early information on the content and transportation needs, some of the uncertainties in the transit process can be reduced. This would result in a smaller value of  $\text{Var}(x)$ .

Fourth, the use of e-seals and tracking data together with Customs' 24 hour rule will allow the manufacturers DC to have advanced information on whether the shipment will be inspected or not. Therefore, part of the uncertainty about the replenishment lead time is resolved at the very beginning of the lead time itself. This results in a decrease of the DC's safety stock requirements. To see this, Hau L. Lee further developed the economic model, given in Appendix C, for safety stock requirements with and without the visibility technology (Lee 2003).

Figure 13 summarizes the various cost savings as a result of enhanced supply chain visibility.

Figure 13: Cost Savings Categories (Lee 2003)

Cost Category	Cost Elements	Comments
Bill of Lading Compliance	- Direct labor cost savings - In-transit inventory reduction due to more efficient bill of lading transmission process	These savings are independent of the amount of inspections carried out at the port of entry, and is a function of how much the current process has already been automated.
Tracking Efficiency	- Reduction in inspection cost - Reduction in pilferage - In-transit inventory reduction due to less inspection	These savings depend on how much reduction of inspection that Customs will give for Greenlane treatment. Pilferage reduction is due to tighter monitoring of the in-transit process.
Supply Chain Confidence	- Safety stock reduction as a result of reduction in the mean and variance of lead time - Safety stock reduction as a result of transparency of advanced lead time information	These savings depend on how much reduction in the mean and variance of lead time can be achieved by SST. The manufacturer should also have advanced scientific inventory control system in place to take advantage of such improvements.

Hau Lee uses some data from a high tech manufacturer participating in the Smart and Secure Tradelanes initiative. The tradelane considered is from Malaysia, Singapore to Seattle, Washington. The average value of goods in a forty equivalent unit (FEU) container used for the case study was \$300,000. The average value of a FEU container in 1998 was \$62,000 (PMA 1999). Through increasing inspection levels on cargo not certified by C-TPAT and not implementing new security technologies, Lee shows cost avoidance and savings of upwards of \$4,000 per container (Lee 2003).

### **Smuggling and Theft Losses**

Depending on the value and type of inventory, many shippers contend with pilferage of contents from containers and the outright disappearance of containers. It is assumed that this solution will reduce pilferage incidents by acting as a deterrent.



Additionally, when pilferage does occur, the attached RFID tag should immediately transmit an emergency signal. Notification allows the shipper and carrier to take immediate action to either stop the act in progress or begin dealing with the disruption. The system can pinpoint the exact location where the intrusion occurred, and, as a result, the shipper has a greater understanding of the supply chain's vulnerabilities.

Worldwide, cargo crimes account for estimated direct merchandise losses of as much as \$50 billion per year (Bangsberg 2000). Lou Tyska, the Chairman of the National Cargo Security Council, claims in the United States alone, cargo theft is estimated to account for as much as \$25 billion in direct merchandise losses per year. Contraband tobacco is a major profit center for international organized crime groups. The global market for smuggled cigarettes is estimated to total \$16 billion per year in lost tax revenues (Mutschke 2000). An FIA international research (Crary 2002) estimates that about one tenth of those losses, or an estimated \$1.75 billion, are incurred in the United States.

These are figures effecting both the public and private sectors, and could be dramatically reduced with tighter container security. A majority of these losses could be recovered or prevented if container movement were tracked through the entire supply chain and anti-tampering devices such as e-seals were used to detect tampering or theft attempts.

### **Enhanced Efficiency Savings**

Since importers and exporters drive typical supply chain service provider relationships, the focus of the Smart and Secure Tradelanes (SST), Phase One analysis was on the costs and benefits to this important constituency. Based on Phase One economic modeling, the general conclusion is that active RFID is a deployable and affordable

technology that is suitable for a global supply chain security and efficiency network (SST 2003).

The SST study found that a single end-to-end move of a typical container nets \$378 - \$462 of potential value to the shipper when subtracting the operating and variable costs. This amounts to 0.52% – 0.66% as a percentage of average total container value shipped in SST, Phase One. The per container potential benefit ranges to a typical shipper are summarized in Table 8:

**Table 8 – Potential Benefits of Enhanced Efficiency (SST 2003)**

<b>Area of Potential Benefit</b>	<b>Percentage of Potential Benefit</b>	<b>Potential Benefit per Container</b>
Reduction in Safety Stock	.25% - .30%	\$173 - \$211
Reduction in Pipeline Inventory	.13% - .16%	\$91 - \$111
Reduction of Service Charges	0.08% - 0.10%	\$56 - \$68
Administrative Labor	0.04% - 0.05%	\$31 - \$38
Reduction of Pilferage, Inspections, Loss	0.04% - 0.05%	\$28 - \$34
<b>Total</b>	<b>0.54% - 0.66%</b>	<b>\$378 - \$462</b>

The model used to develop this table assumes that the average cargo value of a FEU container is \$70,000. This assumption, as compared to Hau Lee’s previously mentioned, better reflects the industry as a whole. Operational benefits will be higher for shipments valued over \$70,000. However, low-value commodities will not derive nearly as much meaningful economic benefit.

**Summary**

The financial models and theory provided in this chapter support the economic benefits incurred from implementing technology to enhance supply chain visibility and efficiency. These are critical results because they produce a win-win scenario for both

security and logistics. The costs of implementing such technology are offset and exceeded by the savings and additional costs avoided when the integrity of the container is maintained and the efficiency and velocity at which it moves through the supply chain are increased. The models and cost estimates maintain the approximate net benefit of \$300 to \$800 per container shipment imported into the United States.

Companies importing goods into the United States should realize impressive financial benefits by utilizing technology to secure, track, and manage their supply chains. These benefits include:

- Improvement in visibility from better predictability and timeliness of cargo shipments
- Cost avoidance related to emerging U.S. Customs' trade security measures
- Reductions in safety stock and inventory carrying costs from improvements in trade compliance and in-transit visibility
- Improvement in customer service to sales channels and re-sellers
- Profit increases from improved product in-stock rates
- Reductions in incidences and direct costs of theft and pilferage

The majority of these result from greater supply chain visibility, transparency, and process improvements, which will allow importers to reduce transit time variations and inventory safety stocks.

## CHAPTER 8: CONCLUSION

### Summary

The research in this thesis has provided a theoretical and analytical outlook on the most promising solution to enhancing container security. The solutions presented for improving security are encouraging not only for protecting the interests of the United States, but the rest of the world as well. The incentive of realized savings for the private sector provides the platform for reform.

As established, the container industry requires a solution which does not impede the flow of commerce but significantly improves the security of the system. The vulnerabilities have been pointed out and the lack of container security around the world is still apparent.

The action taken thus far by both the public and private sectors to pursue the security of the container industry should be applauded. The initiatives and reform already in place are just the first steps towards the overall solution. The results are not only encouraging but promising as well.

Supply chain management is becoming an increasingly more important business function and method for corporations to gain a competitive advantage. Companies who are innovative and effective in supply chain management have shown great success in the past decade. Companies such as Wal-mart and Dell are two good examples of this theory. Due to the ever increasing role of supply chains and their importance, it will only be a matter of time before businesses implement technologies suggested as security solutions to

enhance their visibility and control of the entire supply chain end-to-end. However, the public sector must be extremely careful not to force the technology before it is ready.

Public and private sector leaders must make judgments about when new or improved security products and processes are sufficiently stable and cost-effective to merit implementation and possibly regulatory mandates. The ongoing set of pilot tests and demonstrations are excellent tools to evaluate technology, and develop effective operating procedures and industry best practices. Enabling the technology to work successfully requires consistent and coherent international standards. Countries must not make this an individual effort, rather it must be a globally coordinated and aligned approach. These standards must be flexible enough to accommodate both a growing installed base and continuous upgrades. The public sector must not rush into premature regulations. Implementation of this technology before it is fully tested and developed could result in a failure over the long run.

The network effect, the phenomenon whereby a service becomes more valuable as more people use it, thereby encouraging ever-increasing numbers of adopters, presents both barriers and opportunities for the implementation of the suggested security system. The system's early cost will be high, but unit cost drop dramatically as utilization increases. Simultaneously as the cost drops the security solution will become a more valuable resource as infrastructure is built throughout the world.

To address the solution, the three areas of information, physical security, and inspections must all be enhanced. This thesis has demonstrated the need and effective approach to improving all three aspects. The ability of the information system to support

the technology and analyze the information is the most critical factor to an effective risk management approach. The capabilities and capacities of the information systems must be the strongest link in this chain of integrated technologies.

However, the ultimate question that must be answered is what if a terrorist group takes advantage of the current international trade system by placing a large, devastating weapon inside a shipping container bound for the United States? What is it worth to the government, the economy, and the public to reduce the chance of such an event occurring? The cost of lives, property, and economic decline that would result from an attack using a WMD delivered to the United States by a shipping container would be catastrophic. That is why both the public and private sectors must take any action necessary to help protect our homeland from another terrorist attack.

Overreactions to terrorist attacks can be extremely harmful indirect secondary impacts. As supply chain security expert Steven Flynn pointed out, we must frame debate so that inevitable security breakdowns are treated as military losses in the course of an extended war, not as triggers for counterproductive overreaction (Flynn 2003).

While the benefits from increased supply chain efficiencies make the deployment of this solution advantageous to importers in the United States, the benefits the solution provides to transportation security are the most valuable.

### **Recommendations for Future Work**

There are risks associated with certifying companies such as the members of C-TPAT. Terrorists could use such preferential treatment to avoid Customs detection. Therefore, auditing procedures and funding for such activities must be refined. Another

vulnerability could be the actual manufacturing firms, which stand at the beginning of the supply chain and are just upstream from the first logistics process initiated to move the product through the chain. These manufacturing sites must be a certified credible source and actively participate in security measures because if a terrorist were to penetrate the supply chain at the manufacturing level it may be the most effective way to go undetected.

Furthermore, MIT faculty identified a “Conundrum of Security vs. Standardization” which states that tighter security standards also create new security risks. Every security advance will carry the seeds of another problem (MIT-CTL 2001).

Finally, the “Conundrum of Security vs. Standardization” also pointed out that impacts will be asymmetric, as the costs and benefits fall unequally on firms, and communities (MIT-CTL 2001). The regionalized impacts of container security should be investigated in greater depth.

## WORKS CITED

Albright, Madeleine, "Speech to the Customs College in Tashkent", Testimony on behalf of the U.S. Embassy Uzbekistan, April 2001. (Albright 2001)

APEC, "STAR-BEST Project, Cost – Benefit Analysis", Bearing Point, November 2003. (APEC 2003)

ARC Strategies, "Trade Security: A Wild Card in Supply Chain Management", September 2002. (ARC 2002)

Associated Press, "Liberia Signs Pact to Allow U.S. Navy to Search Ships", February 2004. (AP 2004)

Bangsberg, P. T., "IMB Steps Up Fight Against Cargo Theft", Journal of Commerce, July 2000. (Bangsberg 2000)

Binnendijk, Hans, Leigh C. Caraher, Timothy Coffey, and H. Scott Wynfield, "The Virtual Border: Countering Seaborne Container Terrorism", Defense Horizons, August 2002. (Binnendijk 2002)

Bowser, Gary F., Huseman, Richard C., "Advanced Technology for Security and Customs Enforcement", Port Technology International, August 2002. (Bowser 2002)

Brown, Douglas R., Botello, Steven D., "Automatic Cargo Inspection", Port Technology International, October 2002. (Brown 2002)

Bryant, Dennis L., "Cargo and Maritime Security", Holland & Knight, January 2003. (Bryant 2003)

Center for Transportation and Logistics, "Conundrum: Security vs. Standardization", Massachusetts Institute of Technology, November 2001. (MIT-CTL 2001)

Crary, David, "More Smuggling and Tax Evasion Expected as State After State Hikes Cigarette Taxes", Associated Press, July 2002. (Crary 2002)

Davey, Neil, "Port Security and a Successful Supply Chain", Border and Transportation Security America, February 2002. (Davey 2002)

Flynn, Dr. Stephen E., "The Fragile State of Container Security", Testimony on behalf of the Council on Foreign Relations, March 2003. (Flynn 2003)



General Accounting Office (GAO), “Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors”, Report to Congressional Requesters, July 2003. (GAO 2003)

Gerencser, Mark, Jim Weinberg, and Don Vincent, “Port Security War Games: Implications for U.S. Supply Chains”, Booz, Allen and Hamilton, October 2002. (Gerencser 2002)

Hollings, Senator Ernest F. (D-SC), “Seaport Vulnerability”, Testimony on behalf of the Committee on Government Affairs, December 2001. (Hollings 2001)

Koch, Christopher, “Remarks before the Trans-Pacific Maritime Conference”, The World Shipping Council, March 2004. (Koch 2004)

Koch, Christopher, “Testimony before the Senate Committee on Commerce, Science, and Transportation”, The World Shipping Council, February 2002. (Koch 2002)

Lanier, Robin, “In-bound Container Movement”, Waterfront Coalition, January 2002. (Lanier 2002)

Lecoindre, Franck, Ogier, Catherine, “Trade Facilitation and Illegal Trafficking: By Heimann Cargo Vision”, Port Technology International, November 2002. (Lecoindre 2002)

Lee, Hau L, Whang, Seungjin, “Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management”, Graduate School of Business, Stanford University, July 2003. (Lee 2003)

Lloyd’s Register, “What is the ISPS Code?”, December 2002. (Lloyd’s 2002)

McBee, Christopher J., Bowlin, David W., Orphan, Victor J., “Mobile Cargo Inspection Provides Improved Throughput Efficiency and Flexibility”, Port Technology International, March 2002. (McBee 2002)

Mutschke, Ralf, “Testimony before the House of Representatives Judiciary Subcommittee on Crime”, Criminal Intelligence Directorate, July 2000. (Mutschke 2000)

Nelson, Mark, “Smart and Secure Tradelane Initiative, Press Release”, Savi Technology, July 2002. (Nelson 2002)

O’Hanlon, Michael, et al., “Protecting the American Homeland: A Preliminary Analysis”, Brookings Institution, April 2002. (O’Hanlon 2002)

Operation Safe Commerce – Boston a Model Port, “Interim Project Report”, April 2003. (OSC 2003)

Orient Overseas Container Line Limited, “U.S. Customs 24-hour Advanced Cargo Manifest Declaration Rule”, December 2002. (OOCL 2002)

Pacific Maritime Association, “Import Containers Surge on West, East, and Gulf Coasts”, Volume 11, Number 11, November 1999. (PMA 1999)

Peters, Katherine McIntire, “Seeking Safe Harbors”, Government Executive Magazine, March 2001. (Peters 2001)

Ridge, Secretary Tom, Remarks at the Port of Newark, New Jersey, June 2003. (Ridge 2003)

Ross, Brian, Rhonda Schwartz, and David Scott, “How Safe Are Our Borders?”, ABCNews, September 2003. (Ross 2003)

Rosynsky, Paul T., “Judge Ends Lockout, Union Chafes at Federal Intervention in Port Dispute”, San Mateo County Time, October 2002. (Rosynsky 2002)

Sahagun, Louis, “Really Big Doings at the Ports”, The Los Angeles Times, March 2002. (Sahagun 2002)

Sheridan, Ralph, “Report on Non-Intrusive Inspection Technologies”, U.S. Treasury Advisory Committee on Commercial Operations of the United States Customs Service, June 2002. (Sheridan 2002)

Silver, E., Pyke, D., and Peterson, R., “Inventory Management and Production & Planning Scheduling”, Third Edition, John Wiley & Sons, 1998. (Silver 1998)

Smart & Secure Tradelanes, “Network Visibility: Leveraging Security and Efficiency in Today’s Global Supply Chains”, Phase One Review, November 2003. (SST 2003)

Snell, Michael P., “Gamma Ray Technology”, Port Technology International, November 2002. (Snell 2002)

Steigman, David, “DOT and Customs Launch ‘Operation Safe Commerce’ Program”, TSA, November, 2002. (Steigman 2002)

Strategic Council on Security Technology, “Smart and Secure Tradelanes, An Overview”, May 2003. (SST 2003)

United States Congress, “Maritime Transportation Security Act of 2002, P.L. 107-295”, Sec. 101: Findings, 101 Stat. 2066, November 2002. (Congress 2002)

United States Customs, “Automated Targeting System, A Decision Support Tool”, Office of Field Operations and Technical Support, January 2003. (USCBP 2003)

United States Customs, “Customs – Trade Partnership Against Terrorism Fact Sheet”, United States Customs Service, June 2002. (USCBP 2002)

United States Customs, “Regulatory Information and Security Updates”, Container Security Initiative, January, 2002. (USCBP 2002)

Williscroft, Jason, “Shipping Container Security”, Hotquant, LLC, February 2003. (Williscroft 2003)

Wolfe, Michael, “Freight Transportation Security and Productivity, Executive Summary”, North River Consulting Group, April 2001. (Wolfe 2001)

Wolfe, Michael, “Technology to Enhance Freight Transportation, Security, and Productivity”, Intermodal Freight Security and Technology Workshop, April 2002. (Wolfe 2002)

## WORKS CONSULTED

Alliance Management Group, "In-bound Container Movement, International Ocean Transportation", Waterfront Coalition, January 2002.

Australian Department of Foreign Affairs and Trade, "Costs of Maritime Terrorism and Piracy and the Benefits of Working Together", Economic Analytical Unit, September 2003.

Bearing Point, "Preparing for Further Globalization with RFID", RFID in Retail, November 2003.

Department of Homeland Security, "Protecting America's Ports", Maritime Transportation Security Act of 2002, July 2003.

Hekcer JayEtta Z., "Current Efforts to Detect Nuclear Materials, New Initiative, and Challenges", United States General Accounting Office, November 2002.

General Accounting Office, "Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection", Department of Homeland Security, March 2004.

Green, Anitra, "Secure Container Transport", International Transport Journal, September 1998.

Jackson, Joab, "The Little Chip that Could", Washington Technology, March 2003.

Kenealy, Bill, "Company Offering Cost-Effective Way to Thwart Pilferage", Florida Shipper, September 1998.

Koch, Christopher, "Maritime Security and International Trade", World Shipping Council, July 2002.

Lambright, Stephen, "Smart and Secure Tradelanes", Presentation Given at the U.S. Maritime Security Expo, October 2003.

Lee, Hau, and Wolfe, Michael, "Supply Chain Security Without Tears", Supply Chain Management Review, January 2003.

Mewhirter, Erin, and Fullerton, Michael, "The Trade Act of 2002, What Does It All Mean?", November 2002.

Raine, George, "Longshore Union Blames Owners for Port Backlog", San Francisco Gate, October 2002.

Reese, Andrew K., "Building the Secure Supply Chain", iSource, June 2003.

Sinai, Dr. Joshua, "An Overview and Future Trends in Worldwide Maritime Terrorism", ANSER, October 2003.

Stephens, Richard, "Best Business Practices for Securing America's Borders", Testimony to Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security, July 2003.

"West Coast Ports Silent", Washington Post, October 2002.

Wolfe, Michael, "Technology for Supply Chain Security and Productivity", The North River Consulting Group, September 2003.

Woolever, Gerald, "Guaranteeing Smooth Sailing for Port Security", Homeland Defense Journal, January 2003.

## **APPENDICES**

## **Appendix A: C-TPAT Guidelines**

## IMPORTERS

Develop and implement a sound plan to enhance security procedures throughout your supply chain. Where an importer does not control a facility, conveyance or process subject to these recommendations, the importer agrees to make every reasonable effort to secure compliance by the responsible party. The following are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Procedural Security:** Procedures should be in place to protect against unmanifested material being introduced into the supply chain. Security controls should include the supervised introduction/removal of cargo, the proper marking, weighing, counting and documenting of cargo/cargo equipment verified against manifest documents, the detecting/reporting of shortages/overages, and procedures for verifying seals on containers, trailers, and railcars. The movement of incoming/outgoing goods should be monitored. Random, unannounced security assessments of areas in your company's control within the supply chain should be conducted. Procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected, or suspected, by the company should also be in place.

**Physical Security:** All buildings and rail yards should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include perimeter fences, locking devices on external and internal doors, windows, gates and fences, adequate lighting inside and outside the facility, and the segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged or otherwise fenced-in area.

**Access Controls:** Unauthorized access to facilities and conveyances should be prohibited. Controls should include positive identification all employees, visitors, and vendors. Procedures should also include challenging unauthorized/unidentified persons.

**Personnel Security:** Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

**Education and Training Awareness:** A security awareness program should be provided to employees including the recognition of internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should offer incentives for active employee participation in security controls.

**Manifest Procedures:** Companies should ensure that manifests are complete, legible, accurate, and submitted in a timely manner to Customs.

**Conveyance Security:** Conveyance integrity should be maintained to protect against the introduction of unauthorized personnel and material. Security should include the physical search of all readily accessible areas, the securing of internal/external compartments and panels, and procedures for reporting cases in which unauthorized personnel, unmanifested materials, or signs of tampering, are discovered.



## **BROKERS**

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Procedural Security:** Companies should notify Customs and other law enforcement agencies whenever anomalies or illegal activities related to security issues are detected or suspected.

**Documentation Processing:** Brokers should make their best efforts to ensure that all information provided by the importer/exporter, freight forwarder, etc., and used in the clearing of merchandise/cargo, is legible and protected against the exchange, loss or introduction of erroneous information. Documentation controls should include, where applicable, procedures for:

- Maintaining the accuracy of information received, including the shipper and consignee name and address, first and second notify parties, description, weight, quantity, and unit of measure (i.e. boxes, cartons, etc.) of the cargo being cleared.
- Recording, reporting, and/or investigating shortages and overages of merchandise/cargo.
- Safeguarding computer access and information.

**Personnel Security:** Consistent with federal, state, and local regulations and statutes, companies should establish an internal process to screen prospective employees, and verify employment applications. Such an internal process could include background checks and other tests depending on the particular employee function involved.

**Education and Training Awareness:** A security awareness program should include notification being provided to Customs and other law enforcement agencies whenever anomalies or illegal activities related to security are detected or suspected. These programs should provide:

- Recognition for active employee participation in security controls.
- Training in documentation fraud and computer security controls.

## MANUFACTURERS

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case by case basis depending on the company's size and structure and may not be applicable to all. The company should have a written security procedure plan in place that addresses the following:

**Physical Security:** All buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include:

- Adequate locking devices for external and internal doors, windows, gates, and fences.
- Segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged, or otherwise fenced-in area.
- Adequate lighting provided inside and outside the facility to include parking areas.
- Separate parking area for private vehicles separate from the shipping, loading dock, and cargo areas.
- Having internal/external communications systems in place to contact internal security personnel or local law enforcement police.

**Access Controls:** Unauthorized access to the shipping, loading dock and cargo areas should be prohibited. Controls should include:

- The positive identification of all employees, visitors and vendors.
- Procedures for challenging unauthorized/unidentified persons.

**Procedural Security:** Measures for the handling of incoming and outgoing goods should include the protection against the introduction, exchange, or loss of any legal or illegal material. Security controls should include:

- Having a designated security officer to supervise the introduction/removal of cargo.
- Properly marked, weighed, counted, and documented products.
- Procedures for verifying seals on containers, trailers, and railcars.
- Procedures for detecting and reporting shortages and overages.
- Procedures for tracking the timely movement of incoming and outgoing goods.
- Proper storage of empty and full containers to prevent unauthorized access.
- Procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.

**Personnel Security:** Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

**Education and Training Awareness:** A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining product integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

## WAREHOUSES

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all. Warehouses as defined in this guideline are facilities that are used to store and stage both Customs bonded and non-bonded cargo. The company should have a written security procedure plan in place addressing the following:

**Physical Security:** All buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include:

- Adequate locking devices for external and internal doors, windows, gates and fences.
- Adequate lighting provided inside and outside the facility to include parking areas.
- Segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged, or otherwise fenced-in area.
- Separate parking area for private vehicles separate from the shipping, loading dock, and cargo areas.
- Having internal/external communications systems in place to contact internal security personnel or local law enforcement police.

**Access Controls:** Unauthorized access to facilities should be prohibited. Controls should include:

- The positive identification of all employees, visitors, and vendors.
- Procedures for challenging unauthorized/unidentified persons.

**Procedural Security:** Procedures should be in place to protect against unmanifested material being introduced into the warehouse. Security controls should include:

- Having a designated security officer to supervise the introduction/removal of cargo.
- Properly marked, weighed, counted, and documented cargo/cargo equipment verified against manifest documents.
- Procedures for verifying seal on containers, trailers, and railcars.
- Procedures for detecting and reporting shortages and overages.
- Procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.
- Proper storage of empty and full containers to prevent unauthorized access.

**Personnel Security:** Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

**Education and Training Awareness:** A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

## AIR CARRIERS

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Conveyance Security:** Aircraft integrity should be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security procedures should include the physical search of all readily accessible areas, securing all internal/external compartments and panels, and reporting cases in which unmanifested materials, or signs of tampering, are discovered.

**Access Controls:** Unauthorized access to the aircraft should be prohibited. Controls should include the positive identification of all employees, visitors and vendors as well as procedures for challenging unauthorized/unidentified persons.

**Procedural Security:** Procedures should be in place to protect against unmanifested material being introduced aboard the aircraft. Security controls should include complete, accurate and advanced lists of international passengers, crews, and cargo, as well as a positive baggage match identification system providing for the constant security of all baggage. All cargo/cargo equipment should be properly marked, weighed, counted, and documented under the supervision of a designated security officer. There should be procedures for recording, reporting, and/or investigating shortages and overages, and procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the carrier.

**Manifest Procedures:** Companies should ensure that manifests are complete, legible, accurate, and submitted in a timely manner to Customs.

**Personnel Security:** Employment screening, application verifications, the interviewing of prospective employees and periodic background checks should be conducted.

**Education and Training Awareness:** A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

**Physical Security:** Carrier's buildings, warehouses, and on & off ramp facilities should be constructed of materials which resist unlawful entry and protect against outside intrusion. Physical security should include adequate locking devices for external and internal doors, windows, gates and fences. Perimeter fencing should also be provided, as well as adequate lighting inside and outside the facility; including parking areas. There should also be segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by means of a safe, cage, or otherwise fenced-in area.

## SEA CARRIERS

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Conveyance Security:** Vessel integrity should be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security should include the physical search of all readily accessible areas, the securing all internal/external compartments and panels as appropriate, and procedures for reporting cases in which unmanifested materials, or signs of tampering, are discovered.

**Access Controls:** Unauthorized access to the vessel should be prohibited. Controls should include the positive identification of all employees, visitors, and vendors. Procedures for challenging unauthorized/unidentified persons should be in place.

**Procedural Security:** Procedures should be in place to protect against unmanifested material being introduced aboard the vessel. Security procedures should provide for complete, accurate and advanced lists of crews and passengers. Cargo should be loaded and discharged in a secure manner under supervision of a designated security representative and shortages/overages should be reported appropriately. There should also be procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected, or suspected, by the company.

**Manifest Procedures:** Manifests should be complete, legible, accurate and submitted in a timely manner pursuant to Customs regulations.

**Personnel Security:** Employment screening, application verifications, the interviewing of prospective employees and periodic background checks should be conducted.

**Education and Training Awareness:** A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

**Physical Security:** Carrier's buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include adequate perimeter fencing, lighting inside and outside the facility, and locking devices on external and internal doors, windows, gates, and fences.

## LAND CARRIERS

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Conveyance Security:** Integrity should be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security procedures should include the physical search of all readily accessible areas, securing all internal/external compartments and panels, and procedures for reporting cases in which unmanifested materials, or signs of tampering, are discovered.

**Physical Security:** All carrier buildings and rail yards should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include adequate locking devices on external and internal doors, windows, gates and fences. Perimeter fencing should be addressed, as well as adequate lighting inside and outside the facility, to include the parking areas. There should be segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged or otherwise fenced-in area.

**Access Controls:** Unauthorized access to facilities and conveyances should be prohibited. Controls should include the positive identification of all employees, visitors, and vendors as well as procedures for challenging unauthorized/unidentified persons.

**Procedural Security:** Procedures should be in place to protect against unmanifested material being introduced aboard the conveyance. Security controls should include the proper marking, weighing, counting, and documenting of cargo/cargo equipment under the supervision of a designated security representative. Procedures should be in place for verifying seals on containers, trailers, and railcars, and a system for detecting and reporting shortages and overages. The timely movement of incoming and outgoing goods should be tracked and there should be procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.

**Manifest Procedures:** Companies should ensure that manifests are complete, legible, accurate, and submitted in a timely manner to Customs.

**Personnel Security:** Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

**Education and Training Awareness:** A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

## **AIR FREIGHT CONSOLIDATORS/ OCEAN TRANSPORTATION INTERMEDIARIES, AND NVOCCS**

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

**Procedural Security:** Companies should notify Customs and other law enforcement agencies whenever anomalies or illegal activities related to security issues are detected or suspected.

**Documentation Processing:** Consolidators should make their best efforts to ensure that all information provided by the importer/exporter, freight forwarder, etc., and used in the clearing of merchandise/cargo, is legible and protected against the exchange, loss or introduction of erroneous information. Documentation controls should include, where applicable, procedures for:

- Maintaining the accuracy of information received, including the shipper and consignee name and address, first and second notify parties, description, weight, quantity, and unit of measure (i.e. boxes, cartons, etc.) of the cargo being cleared.
- Recording, reporting, and/or investigating shortages and overages of merchandise/cargo.
- Tracking the movement of incoming and outgoing cargo.
- Safeguarding computer access and information.

Companies should participate in the Automated Manifested System (AMS) and all data submissions should be complete, legible, accurate and submitted in a timely manner pursuant to Customs regulations.

**Personnel Security:** Consistent with federal, state, and local regulations and statutes, companies should establish an internal process to screen prospective employees, and verify applications. Such an internal process could include background checks and other tests depending on the particular employee function involved.

**Education and Training Awareness:** A security awareness program should include notification being provided to Customs and other law enforcement agencies whenever anomalies or illegal activities related to security are detected or suspected. These programs should provide:

- Recognition for active employee participation in security controls.
- Training in documentation fraud and computer security controls.

**Appendix B: Port Security Grant Program Funding**



# U. S. DEPARTMENT OF HOMELAND SECURITY

## Transportation Security Administration

### Protecting Our Ports

#### Operation Safe Commerce and Port Security Grants



**U. S. DEPARTMENT OF HOMELAND SECURITY  
Transportation Security Administration**

---

**Port Security Grant Program**

<b>Grantee Name</b>	<b>City</b>	<b>State</b>	<b>Total Value</b>
Port of Homer	Homer	AK	\$167,000
AK Depart of Transportation & Public Facilities	Juneau	AK	\$2,235,000
City and Borough of Juneau Engineering Department	Juneau	AK	\$131,265
City of Ketchikan	Ketchikan	AK	\$62,500
Alaska Railroad Corporation	Seward	AK	\$437,000
SouthEast Stevedoring Corporation	Skagway	AK	\$249,990
Petro Star Inc.	Valdez	AK	\$513,500
CSX Lines	Kodiak/San Juan	AK/PR	\$175,000
Shell Chemical LP	Mobile	AL	\$175,000
Alabama State Port Authority	Mobile	AL	\$773,000
Benicia Port Terminal Company	Benicia	CA	\$20,000
Harbor Dept. of the City of Long Beach	Long Beach	CA	\$9,820,000
City of Long Beach	Long Beach	CA	\$200,163
Total Terminals International Pier T Long Beach	Long Beach	CA	\$665,000
City of Los Angeles, Los Angeles Harbor Department	Los Angeles	CA	\$800,000
Trans Pacific Container Service Corp.	Los Angeles	CA	\$1,189,961
Pacific Harbor Line, Inc.	Los Angeles	CA	\$95,000
Alameda Corridor Transportation Authority	Los Angeles	CA	\$1,440,000
Vopak Terminal Los Angeles Inc.	Los Angeles	CA	\$1,070,000
West Basin Container Terminal, Inc.	Los Angeles	CA	\$1,246,000
Seaside Transportation Services, Port of L.A.	Los Angeles	CA	\$1,754,650
Shell Oil Products, U.S. Martinez Refinery	Martinez	CA	\$200,000
Port of Oakland	Oakland	CA	\$1,600,000

Total Terminals International Berth 55-56 Oakland	Oakland	CA	\$476,000
Seaside Transportation Services, Port of Oakland	Oakland	CA	\$376,000
Port of Redwood City	Redwood City	CA	\$75,000
Port of Richmond, California	Richmond	CA	\$91,000
San Diego Unified Port District	San Diego	CA	\$1,435,750
Red and White Fleet	San Francisco	CA	\$41,450
Port of San Francisco	San Francisco	CA	\$3,375,000
Golden Gate Bridge, Highway and Transportation Dis	San Francisco	CA	\$520,000
Stockton Port District	Stockton	CA	\$336,204
California Ammonia Company	Stockton	CA	\$150,000
City of Vallejo, California	Vallejo	CA	\$500,000
Eagle Marine Services, Ltd.	Los Angeles/Oakland/Seattle	CA/WA	\$1,034,000
Motiva Enterprises LLC	Bridgeport	CT	\$240,336
Consumers Petroleum of Ct., Inc	Bridgeport	CT	\$22,400
Hoffman Fuel Company of Bridgeport Inc	Bridgeport	CT	\$20,000
New Haven Terminal, Inc.	New Haven	CT	\$446,761
Williams Energy Partners	New Haven	CT	\$430,000
State of Connecticut	New Haven	CT	\$75,000
Motiva Enterprises LLC	New Haven	CT	\$298,727
City of New Haven, Connecticut	New Haven	CT	\$171,312
Gateway Terminal	New Haven	CT	\$43,500
Nelseco Navigation Company	New London	CT	\$17,500
Cross Sound Ferry Services Inc.	New London	CT	\$56,926
Heating Oil Partners LP DDLC Energy	New London	CT	\$38,500
Fishers Island Ferry District	New London	CT	\$300,000

Getty Terminals Corp.	New Haven/ Newark/Providence	CT/NJ/RI	\$195,435
Spirit Marine Incorporated	Washington/New York	DC/NY	\$58,485
Motiva Enterprises, LLC	Deleware City	DE	\$196,200
City of Delaware City - Police Department	Deleware City	DE	\$94,200
Canaveral Port Authority	Cape Canaveral	FL	\$535,000
Ocean Highway and Port Authority	Fern Beach	FL	\$58,590
G&G Shipping, Inc	Ft. Lauderdale	FL	\$225,000
Broward County Board of County Commissioners	Ft. Lauderdale	FL	\$639,059
Jacksonville Seaport Authority aka JAXPORT	Jacksonville	FL	\$962,752
Support Terminals Operating Partnership, L.P.	Jacksonville	FL	\$384,000
Dante B. Fascell Port of Miami-Dade	Miami	FL	\$7,581,206
Port of Palm Beach District	Palm Beach	FL	\$261,072
Manatee County Port Authority	Palmetto	FL	\$2,280,246
Coastal Fuels Marketing, Inc.	Port Everglades	FL	\$710,000
Tampa Port Authority	Tampa	FL	\$4,000,000
Chatham County	Savannah	GA	\$134,273
CITGO Asphalt Refining Company	Savannah	GA	\$750,000
Southern LNG Inc.	Savannah	GA	\$200,000
Georgia Ports Authority	Savannah	GA	\$1,528,600
ConocoPhillips, Lubricants	Savannah	GA	\$16,770
Matson Navigation Company	Honolulu	HI	\$805,000
The Gas Company, Division of Citizens Communicatio	Honolulu	HI	\$630,561
State of Hawaii - Department of Transportation	Honolulu	HI	\$645,000
Tesoro Hawaii Corporation	Honolulu	HI	\$2,850,000
Chevron Products Company - Hawaii Refinery	Honolulu	HI	\$625,000

State of Hawaii, Dept. of Land & Natural Resources	Kailu Kona	HI	\$1,450,000
Tri-City Regional Port District	Granite City	IL	\$100,000
BASF Corporation	Joliet	IL	\$475,000
Indiana Port Commission	Portage/Jeffersonville/Mt. Vernon	IN	\$68,800
Mississippi County Port Authority	Hickman	KY	\$55,136
Plaquemines Port Harbor & Terminal District	Belle Chasse	LA	\$435,000
LOOP LLC Deepwater Port Complex	Galliano	LA	\$772,390
Shell Chemical LP	Geismar	LA	\$430,137
CITGO Petroleum Corporation, LCMC	Lake Charles	LA	\$13,467,015
PPG Industries, Inc.	Lake Charles	LA	\$600,000
Williams Energy Partners, LP	Marrero	LA	\$155,000
P&O Ports Louisiana, Inc.	New Orleans	LA	\$487,500
Board of Commissioners of the Port of New Orleans	New Orleans	LA	\$665,000
Bunge North America	New Orleans	LA	\$172,500
Motiva Enterprises L.L.C	Norco	LA	\$225,000
Shell Chemical LP	Norco	LA	\$50,000
Greater Lafourche Port Commission	Port Fourchon	LA	\$1,350,000
Caddo-Bossier Parishes Port Commission	Shreveport	LA	\$40,000
Ergon St. James, Inc.	St. James	LA	\$160,000
Venice Energy Services Company, L.L.C.	Venice	LA	\$131,435
Vopak Terminal Westwego Inc.	Westwego	LA	\$750,000
Kinder Morgan Energy Partners, L.P.	Harvey/Chicago/Gelena Park/Newark/Philadelphia	LA/IL/TX/NJ /PA	\$932,121
Massachusetts State Police	Boston	MA	\$1,200,955
Massachusetts Port Authority	Boston	MA	\$1,175,000

Massachusetts Environmental Police	Boston	MA	\$360,000
Distrigas of Massachusetts LLC	Everett	MA	\$300,000
Everett Police Department	Everett	MA	\$170,000
Governor's Seaport Advisory Council	New Bedford/Gloucester/Fall River/Salem	MA	\$100,000
Town of Oak Bluffs Emergency Management Department	Oak Bluffs	MA	\$285,000
Woods Hole Steamship Authority	Woods Hole	MA	\$624,000
Global Companies, LLC	Revere/Portland	MA/ME	\$243,816
Maryland Port Administration	Baltimore	MD	\$3,170,094
CNX Marine Terminals Inc.	Baltimore	MD	\$420,438
City of Baltimore	Baltimore	MD	\$750,000
City of Portland	Portland	ME	\$1,296,000
Maine Port Authority	Searsport/Bar Harbor	ME	\$632,880
City of Ludington Police Department	Ludington	MI	\$35,000
Lake Michigan Carferry	Ludington	MI	\$126,000
BASF Corporation	Hannibal	MO	\$125,000
Mississippi State Port Authority at Gulfport	Gulfport	MS	\$184,194
Port of Pascagoula via Michael J. Kondracki	Pascagoula	MS	\$521,250
North Carolina State Ports Authority	Wilmington	NC	\$4,870,000
Sea-3, Inc.	Newington	NH	\$80,000
International Matex Tank Terminals	Bayonne	NJ	\$486,813
Global Terminal & Container Services, Inc.	Jersey City	NJ	\$75,000
ConocoPhillips Company	Linden	NJ	\$200,000
ST Linden Terminal, LLC	Linden	NJ	\$350,000
waterfront commission of new york harbor	New York	NJ	\$619,294

Motiva Enterprises LLC	Newark	NJ	\$220,000
	Newark/Bayshore/Cape		
New Jersey Department of Transportation	May/Pt. Pleasant	NJ	\$2,291,000
CITGO Petroleum	Paulsboro	NJ	\$450,000
Motiva Enterprises LLC	Sewaren	NJ	\$175,000
K-Sea Transportation Corp	New York	NY	\$169,563
New York City Department of Transportation	New York	NY	\$7,047,500
Maritime Association of the Port of NY/NJ	New York	NY	\$850,000
Circle Line - Statue of Liberty Ferry Inc.	New York	NY	\$15,600
The Port Authority of New York & New Jersey	New York	NY	\$885,000
Canadian American Transportation Systems, LLC	Rochester	NY	\$1,105,000
Cleveland-Cuyahoga County Port Authority	Cleveland	OH	\$400,000
Dow Chemical Co.	Ironton/Huntington	OH	\$175,000
Toledo-Lucas County Port Authority	Toledo	OH	\$202,000
The City of Tulsa - Rogers County Port Authority	Tulsa	OK	\$725,000
Multnomah County Sheriff's Office	Portland	OR	\$675,000
Regional Maritime Security Coalition-Columbia Rive	Portland	OR	\$510,000
Philadelphia Regional Port Authority	Philadelphia	PA	\$1,768,431
Sunoco, Inc. (R&M)	Philadelphia	PA	\$665,000
Sunoco, Inc. (R&M)	Philadelphia	PA	\$1,365,000
Sunoco, Inc.	Philadelphia	PA	\$665,138
Delaware River Port Authority	Philadelphia	PA	\$250,000
Great Lakes Terminal & Transport of PA	Pittsburgh	PA	\$30,000
Sunoco logistics l.p.	Tinicum Township	PA	\$408,400
Peerless Oil & Chemicals, Inc.	Penuelas	PR	\$22,000
Port of Ponce	Ponce	PR	\$125,000

Puerto Rico Ports Authority	San Juan	PR	\$350,000
Crowley Maritime Corporation	San Juan	PR	\$40,000
Demaco Corporation	San Juan	PR	\$25,000
Interstate Navigation Company	Narragansett	RI	\$46,000
ProvPort, Inc.	Providence	RI	\$50,000
TE Products Pipeline Company, Limited Partnership	Providence	RI	\$259,000
South Carolina State Ports Authority	Charleston	SC	\$1,776,889
Spirit Line Cruises - Fort Sumter Tours, Inc.	Charleston	SC	\$51,000
Memphis & Shelby County Port Commission	Memphis	TN	\$639,655
Port of Beaumont Navigation District	Beaumont	TX	\$863,106
Neches Industrial Park, Inc.	Beaumont	TX	\$223,000
Transmontaigne Product Services, Inc.	Brownsville	TX	\$55,500
Port of Corpus Christi Authority	Corpus Christi	TX	\$4,176,281
CITGO Refining and Chemicals Company L.P.	Corpus Christi	TX	\$1,000,000
Brazos River Harbor Navigation District	Freeport	TX	\$701,300
The Dow Chemical Company	Freeport	TX	\$1,425,000
Williams Energy Partners	Galena Park	TX	\$721,327
Port of Galveston	Galveston	TX	\$1,421,000
Vopak Terminal Galena Park Inc.	Galena Park	TX	\$31,875
Port of Houston Authority Harris County Texas	Houston	TX	\$2,540,200
Stolthaven Houston, Inc.	Houston	TX	\$75,000
Port Terminal Railroad Association	Houston	TX	\$1,346,535
Odfjell Terminals (Houston) LP	Houston	TX	\$52,000
Sunoco Partners Marketing & Terminals LP	Nederland	TX	\$1,807,794
Sunoco Chemicals (formerly Airstech Chemical Corp)	Pasadena	TX	\$183,054
Motiva Enterprises, LLC	Port Arthur	TX	\$307,908



Port of Port Lavaca / Point Comfort	Port Lavaca	TX	\$218,050
Port of Texas City	Texas City	TX	\$250,000
Victoria Cnty Navigation Distrct /Port of Victoria	Victoria	TX	\$344,080
City of Chesapeake	Chesapeake	VA	\$170,000
Atlantic Energy, Inc.	Chesapeake	VA	\$214,779
Mid Atlantic Terminals, LLC	Chesapeake	VA	\$414,320
Virginia Marine Resources Commission	Hampton Roads	VA	\$335,000
Virginia Port Authority	Norfolk	VA	\$3,090,400
City of Norfolk	Norfolk	VA	\$193,760
BASF Corporation	Portsmouth	VA	\$54,000
Port of Richmond	Richmond	VA	\$72,000
Virginia Beach Police Department	Virginia Beach	VA	\$506,599
Hovensa LLC	Christiansted	VI	\$1,340,000
V.I. Water & Power Authority	Christiansted	VI	\$197,810
The West Indian Company Limited	St. Thomas	VI	\$335,435
Tesoro Refining and Marketing Company	Anacortes	WA	\$160,000
Port of Port Angeles	Port Angeles	WA	\$100,000
Washington State Ferries	Seattle	WA	\$6,892,588
Port of Seattle	Seattle	WA	\$5,913,436
Clipper Navigation, Inc.	Seattle	WA	\$12,800
Total Terminals International T-46 Seattle	Seattle	WA	\$392,000
City of Tacoma Police Department	Tacoma	WA	\$258,234
Tidewater Barge Lines	Vancouver	WA	\$8,598
SSA Pacific Terminals Inc	Seattle/Los Angeles/Long Beach/Oakland	WA/CA	\$1,699,579

	Tacoma/Baltimore/Elizabeth/ Portsmouth/Charleston/Hous ton/Jacksonville	WA/MD/NJ/ VA/SC/TX/ FL	
APM Terminals North America, Inc.			\$666,000
PPG Industries, Inc.	New Martinsville	WV	\$522,000
		<b>Total</b>	<b>\$169,055,136</b>

**Article I. OPERATION SAFE COMMERCE**

<b>Grantee Name</b>	<b>ST</b>	<b>Total Value</b>
Port of Los Angeles/Long Beach	CA	\$8,250,356
The Port Authority of NY & NJ	NY	\$6,747,227
Port of Seattle/Tacoma	WA	\$13,302,791

**Appendix C: Economic Model for Safety Stock Savings through Visibility and Control  
(Lee 2003)**

Let:

$\mu$  = mean daily demand of product

$\sigma$  = standard deviation of the daily demand of the product

$R$  = inter-replenishment time in days for the DC

$k$  = safety stock factor

$p'$  = new inspection rate with enhanced security and visibility

$1 - \theta$  = percentage reduction of the transit time variance as a result enhanced security and visibility. Hence, the new transit time variance would be given by  $\theta \text{Var}(x)$ .

Without the technology, under the current processes, the safety stock is given by (Silver 1998):

$$S_0 = k\sqrt{\mu^2 \text{Var}(T) + \sigma^2 E(T + R)}$$

With the technology, advanced information about the lead time statistics is obtained, and therefore the safety stock, based on the knowledge of whether inspection is needed or not, could be adjusted. The resulting safety stock is:

$$S_1 = k\left(p'\sqrt{\mu^2 [\theta \text{Var}(x) + \text{Var}(y)] + \sigma^2 [E(x) + E(y) + R]} + (1 - p')\sqrt{\mu^2 \theta \text{Var}(x) + \sigma^2 [E(x) + R]}\right)$$

In order to prove the reduction in safety stock,  $S_1 \leq S_0$ . Let:

$$H_1 = \mu^2 \text{Var}(y) + \sigma^2 E(y) + H_2, \text{ and}$$

$$H_2 = \mu^2 \theta \text{Var}(x) + \sigma^2 [E(x) + R]$$

Then, the expression  $S_0 \geq k\sqrt{pH_1 + (1 - p)H_2}$  can be made, and

$S_1 = k[p'\sqrt{H_1} + (1 - p)\sqrt{H_2}]$ . Note that, for any random variable  $Z$ ,  $\sqrt{E(Z)} \geq E(\sqrt{Z})$ , based on

Jensen's inequality. Hence:

$$S_0 \geq k\sqrt{pH_1 + (1-p)H_2} \geq k[p\sqrt{H_1} + (1-p)\sqrt{H_2}] \geq k[p'\sqrt{H_1} + (1-p)\sqrt{H_2}] = S_1$$

The last inequality above follows from the fact that  $p \geq p'$  and  $H_1 \geq H_2$ .

One of the values of implementing the technology to improve supply chain visibility and security is the advanced information on lead time provided to the manufacturer. This information is more valuable than simply reducing the variance of lead time. This is demonstrated by a simple analysis developed by Hau Lee. Let  $t$  be the random variable denoting the exposure time, and  $\mu$  and  $\sigma$  be the mean and standard deviation of demand per unit time. With advanced knowledge of  $t$ , it is possible that the manufacturer can dynamically adjust the safety stock at each replenishment instance. Without advanced lead time knowledge, the safety stock requirement is  $k\sqrt{\mu^2 \text{Var}(t) + \sigma^2 E(t)}$ , where  $k$  is the safety factor. With advanced lead time knowledge, the average safety stock requirement is  $k\sigma E(\sqrt{t})$ . The safety stock requirement without advanced lead time knowledge is expressed as:

$$k\sqrt{\mu^2 \text{Var}(t) + \sigma^2 E(t)} = k\sqrt{\mu^2 \text{Var}(t) + \sigma^2 [\text{Var}(\sqrt{t}) + (E\sqrt{t})^2]} \geq k\sigma E(\sqrt{t})$$

The difference of the two safety stock requirements is greater with higher values of  $\text{Var}(t)$  and  $\text{Var}(\sqrt{t})$ . With advanced lead time knowledge, safety stock can be reduced not only from the  $\mu^2 \text{Var}(t)$  term, but also the  $\sigma^2 \text{Var}(\sqrt{t})$  term as well.