

PORT SECURITY AND INFORMATION TECHNOLOGY

By

NIKOLAOS HARILAOS PETRAKAKOS

B.S. Naval Architecture and Marine Engineering
Webb Institute, 2004

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

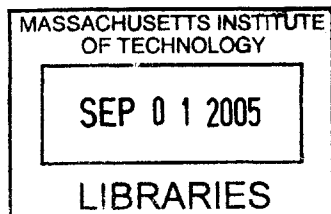
MAY 2005 [Signature]

© 2005 Massachusetts Institute of Technology
All rights reserved

Signature of Author: _____
Department of Ocean Engineering
May 18, 2005

Certified By: _____
Dr. Hauke Kite-Powell
Thesis Supervisor

Accepted by _____
Michael S. Triantafyllou
Director, Center for Ocean Engineering,
Department of Mechanical Engineering



BARKER

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
ABSTRACT.....	3
ACKNOWLEDGEMENTS	4
LIST OF FIGURES AND TABLES	5
CHAPTER 1 – Introduction	6
1.1 - PURPOSE.....	6
1.2 - CONTENT DESCRIPTION.....	8
CHAPTER 2 - Background on Ports and Security	10
2.1 – US PORTS BACKGROUND.....	10
2.2 – US PORT SECURITY MEASURES	12
2.3 – US FEDERAL AGENCY MEASURES	18
2.4 – SECURITY SHORTCOMINGS AS IDENTIFIED BY GAO	20
2.5 – CONCLUSION.....	24
CHAPTER 3 - Generic IT Needs Related to Vessel Arrival.....	26
3.1 – OCEAN DOCUMENTATION DESCRIPTION.....	26
3.2 – OCEAN DOCUMENTATION DESCRIPTION.....	43
CHAPTER 4 - Following the Information Flow of an Export Container	44
4.1 – INTRODUCTION	44
4.2 – STAKEHOLDER ROLES AND RESPONSIBILITIES	45
4.3 – CONTAINER INTERMODAL MOVEMENT	50
4.4 - CONCLUSION	58
CHAPTER 5 - Ports as Information Managers	59
5.1 - INTRODUCTION AND GENERAL CONCERNS	59
5.2.1 - DRMEC – RISK Alert.....	60
5.2.2 PROOF OF CONCEPT DEMONSTRATION	65
5.3.1 Port of NY/NJ – F.I.R.S.T.	70
5.3.2 CONCERNS	73
5.4.1 EMODAL	76
5.4.2 CONCERNS	77
5.5.1 INTERNATIONAL SYSTEMS - PORTNET.....	78
5.6.1 SAVI – SMART CONTAINERS	80
5.7 CONCLUSIONS	82
GLOSSARY OF TERMS AND ABBREVIATIONS	89
BIBLIOGRAPHY	92

PORT SECURITY AND INFORMATION TECHNOLOGY

by

NIKOLAOS HARILAOS PETRAKAKOS

Submitted to the Department of Ocean Engineering
on May 18, 2005 in Partial Fulfillment of the
Requirements for the Degree of Master of Science in
Ocean Systems Management

ABSTRACT

The terrorist attacks of September 11th 2001 on New York and Washington DC shed light on the many security shortcomings that sea ports and the entire import and export process face. A primary source of these problems is the information sharing process which makes it hard to track the source of a problem in the import and export process due to lack of information and coordination. This thesis attempts to examine these data sharing problems by looking at what federal agencies, ports, and other private firms have been doing to solve the problems. The document exchange between various stakeholders and the process behind that was also examined to find potential problems. The reason behind doing this is because it is essential to understand the process and its problems before any meaningful results can be extracted from examining the efforts being done to solve the problems. The findings were similar for all cases showing that the primary reason preventing any of these problems to be solved is the unwillingness of commercial stakeholders to share information due to lack of incentives and privacy concerns.

Thesis Supervisor: Dr. Hauke Kite-Powell
Title: Lecturer

AKNOWLEDGEMENTS

The author wishes to acknowledge the time and assistance provided by those interviewed. The list includes eModal, Karen Tobia (FIRST), and William Shepard (DRMEC). Their patience, suggestions made possible the creation of this thesis. The author also wishes to acknowledge Nortel Networks for the partial financial support provided for this research. It is the author's hope that each of the aforementioned will benefit, either directly or indirectly, from the analysis herein contained.

LIST OF FIGURES AND TABLES

EXHIBIT 2.1.....	13
EXHIBIT 3.1.....	29
EXHIBIT 3.2.....	34
EXHIBIT 3.3.....	35
EXHIBIT 3.4.....	36
EXHIBIT 3.5.....	38
EXHIBIT 3.6.....	39
EXHIBIT 3.7.....	40
EXHIBIT 3.8.....	42
Figure 4.1: Stakeholder Interaction of export process of a container in the US.....	48
Figure 4.2: Stakeholder Interaction of export process of a container in Singapore.....	49
Table 4.1 - Information Exchange for Export Process	53
EXHIBIT 4.1 – Timeline of data exchange for export process of a container	54
EXHIBIT 4.2 – Diagrammatic representation of the Container Documentation Exchange	56
Figure 5.3: Overview of RISK Alert data flow and features	60
Figure 5.4: Sample of Information Flow in RISK Alert.....	61
Figure 5.5: PurpleFinder screenshot	63
Figure 5.6: RISK Alert crewmember information page screenshot	64
Figure 5.7: FIRST Information sources, types, and users.....	71
Figure 5.8: Overview of FIRST.....	72
Table 5.1 - Levels of Access to FIRST System Features2	73

CHAPTER 1 – Introduction

1.1 - PURPOSE

The terrorist attacks on New York and Washington D.C. in 2001 brought to the surface with them many vulnerabilities in the flow of international cargo through all modes of transportation. However, the other modes such as air-traffic, had aspects that were straightforward to identify and upgrade (although requiring significant funding). Since 96 percent of all overseas imports to the US are by sea, it is obvious that an important area of improvement is port security, and anything that is connected to it, which are other modes such as truck and rail as well.

The US government initiated many programs for various funding to US ports, in order to alleviate some of their security shortcomings. However, most of these funds were dedicated towards the repair of fencing, adding patrol boats, and other unsophisticated measures. The real problems however, are not how to prevent unauthorized entry. In case of a terrorist attack using hazardous chemicals or bombs, it is not of much use to prevent people from entering the port, when the container with the bomb is already in port, which is often near a metropolitan area. More efforts have to be placed on the information aspect of security, which is the most effective way of preventing a “bad” container from ever entering the country.

Some ports and other private firms have decided to follow up on this, by developing systems to capture data being shared between stakeholders in the process, in

an attempt to make the flow more visible and a threat more readily detectable.

Government agencies such as the US Coast Guard and US Customs have placed emphasis on data issues as well by performing demonstrations, and implementing several measures to improve security and efficiency of the cargo flow. The focus for both government agencies and ports has been placed on containerized cargo and passenger vessels, which are less of a commodity and harder to control compared to liquid and dry tankers.

The objective of this thesis is to examine the information technology of port security as outlined above, by examining these efforts by ports and government agencies to remove some of the inherent vulnerabilities from the system by trying to manage the data flow, primarily for containerized cargo.

Prior to examining these ports and their efforts, however, it is essential to know what information is actually being exchanged. The basic information flow required prior to a ship's entry in port has to be examined in order to see what is currently being exchanged, and where some of the potential problems could lie. However, since the import and export of a container does not start and end from when a container is loaded onto the ship to when it is unloaded, the entire intermodal chain of information and stakeholders also has to be examined in detail to find other vulnerabilities in the data exchange.

1.2 - CONTENT DESCRIPTION

As mentioned above, this thesis will examine the data being exchanged between stakeholders in the intermodal process of exporting and importing a container. The next chapter starts with some basic background on ports, and what some of the major ports have done since 9/11. I will focus on an approach taken by some ports to collect and manage large amounts of cargo movement-related data (A separate approach would be to communicate specific pieces of this data rather than to collect and manage it; please refer to the thesis by Alexander Sichel on *Supply Chain Security and Information Technology* for further information on this approach). Apart from the ports, efforts by the US Coast Guard to evaluate and improve security issues will be examined as well, through the results of a nationwide demonstration involving US ports and threat assessment tests.

The third chapter examines the documentation that a ship has to send prior to or during arrival in port. Some of these documents, however, rely greatly on the “goodwill” of the ship’s captain or operating firm to send accurate information. Therefore, each of these documents is described in detail.

The fourth chapter discusses the information being exchanged in a grander scale, involving the entire intermodal process of exporting a container from beginning to end, in order to find possible vulnerabilities and areas of improvement. All the data being exchanged among stakeholders in chronological order are examined, as well as the roles and responsibilities of each of these stakeholders.

The fifth chapter examines the information technology systems that have been developed by ports with government funding, or private firms, in order to find common weaknesses and strengths that other ports or private firms could use when developing such systems. The final chapter summarizes the findings in each of the previous chapters and puts these together in order to provide a set of recommendations for future improvements to the export and import process and the security of ports, primarily through the improvement of data exchange and visibility.

CHAPTER 2 - Background on Ports and Security

2.1 – US PORTS BACKGROUND

As usual, for any major development or technological change to take place in the maritime field, a major event has to bring certain vulnerabilities to light. For the tanker industry, the change from single hull to double hull standards was rushed due to the Exxon Valdez grounding (along with other tanker accidents), creating OPA '90 regulations. Today, major changes are being driven by the terrorist attacks on New York and Washington D.C on September 11th, 2001, which has brought to light the major vulnerabilities of US domestic and international ports, which are an integral part of a much larger global transportation system.

Ports are inherently vulnerable due to several factors. The great amount of volume being transported through these ports makes them an easy avenue for terrorist attacks. From 2000 to 2020, container growth is expected to more than double. Container ships have grown from 2000 TEUs (twenty-foot equivalent unit) to 10000 TEUs in the past three decades. Over 95 percent of all US overseas cargo passes through these ports¹. These trends have led many ports to be thinking about expanding in land size or dredging, in order to handle this growth. Their extensive size and easy access by land and water make it difficult to implement security measures that can, for example, be applied to airports. The vicinity of many ports to metropolitan areas poses another serious threat.

¹ *Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention*. United States Government Accountability Office, January 2005

Oil tank farms, hazardous material storage, and other facilities are often located near urban life, roads, bridges, factories, etc. This also leads to the intermodal aspect, since combining so many different modes such as rail and roads, and the handling of people, high value cargo, and hazardous material, make ports lucrative targets for terrorist activities. These vulnerabilities are a result of ports inadequacy to handle the increasing vessels, cargo, and people flowing through. Drugs and illegal aliens are smuggled routinely into the US hidden between legitimate cargoes aboard large commercial vessels due to these vulnerabilities, and can easily be exploited by terrorists to stage their attacks.

However, besides the impact such a terrorist attack can have on the well being of many people living in the vicinity of ports and on the environment, they can result in devastating economic impact. The Brookings Institute estimated that in 2002, a weapon of mass destruction shipped my mail could result in losses reaching as much as one trillion dollars². In 2002, a simulation of a terrorist attack involving containers, included having every seaport being shut down, which resulted in a \$58 billion loss in revenue to the US economy, not including the effects on the international economy³.

² *Protecting the American Homeland: A Preliminary Analysis* by Michael E. O'Hanlon et al., Washington, D.C.: Brookings Institution Press, 2002.

³ *Systems Engineering Approach to Analysis of the United States Critical Infrastructure and US Ports as Subsystems of the Extended Enterprise System*. Susan Vandiver, Southern Methodist University, 2005

2.2 – US PORT SECURITY MEASURES

Due to the aforementioned vulnerabilities, ports have been forced to upgrade their security measures. However, the role of port authorities have been different from port to port, due to different sizes, current situation, funding availability, and managing position. What I mean by managing position is whether a port acts as a landlord or operator port. A landlord port is a port where the port has minimal effect on how each terminal is run, which is left up to the separate terminal operators. This means that the port authority will typically not take it upon itself to implement any complicated and expensive security measures that would affect operations within a terminal. Operator ports are the opposite, since their philosophy is that they are in charge of the port and will take it upon their duties to implement measures beyond the minimum requirements, which will hopefully simultaneously improve the services they offer by improving efficiency. The trend has been for the major ports, such as LA and Long Beach to act as landlord ports, and smaller ports to be operator ports. Exhibit 2.1 shows the top US ports and their landlord or operator stance. This positioning of each port is one factor affecting the different levels of security measures between ports, along with the amount of funding received by each port authority.

EXHIBIT 2.1			
U.S. PUBLIC PORT OPERATING STATUS			
	Landlord	Operating	Limited Operating
Alabama State Port Authority		x	
Albany, Port of			x
Anchorage, Port of	x		
Beaumont, Port of		x	
Bellingham, Port of		x	
Bridgeport Port Authority	x		
Brownsville, Port of	x		
Canaveral Port Authority	x		
Cleveland-Cuyahoga County Port Authority	x		
Coos Bay, Port of	x		
Corpus Christi Authority, Port of			x
Detroit/Wayne County Port Authority	x		
Duluth Seaway Port Authority	x		
Everett, Port of		x	
Freeport, Port of		x	
Galveston, Port of	x		
Georgia Ports Authority		x	
Grays Harbor, Port of		x	
Greater Baton Rouge Port Commission	x		
Greater LaFourche Port Commission	x		
Green Bay, Port of	x		
Guam, Port Authority of		x	
Hawaii DOT, Harbors Division		x	
Houston Authority, Port of			x
Humboldt Bay Harbor District	x		
Iberia, Port of	x		
Indiana Port Commission	x		
Jackson County Port Authority/Port of Pascagoula	x		
Jacksonville Port Authority	x		
Kalama, Port of	x		
Lake Charles Harbor & Terminal District		x	
Long Beach, Port of	x		
Longview, Port of		x	
Los Angeles, Port of	x		
Manatee County Port Authority	x		
Maryland Port Administration			x
Massachusetts Port Authority		x	
Miami, Port of	x		
Milwaukee, Port of		x	
Mississippi State Port Authority, Gulfport	x		

	Landlord	Operating	Limited Operating
New Orleans, Port of	x		
New York/New Jersey, Port Authority of	x		
North Carolina State Ports Authority		x	
Oakland, Port of	x		
Olympia, Port of		x	
Orange, Port of		x	
Oswego Authority, Port of		x	
Oxnard Harbor District/Port Hueneme		x	
Palm Beach District, Port of	x		
Panama City Port authority		x	
Pensacola, Port of	x		
Philadelphia Regional Port Authority	x		
Plaquimines Port, Harbor & Terminal District	x		
Port Angeles, Port of		x	
Port Arthur, Port of		x	
Port Everglades			x
Port Lavaca-Point Comfort, Port of		x	
Portland (OR), Port of			x
Puerto Rico Ports Authority		x	
Redwood City, Port of	x		
Richmond (VA), Port of	x		
Sacramento, Port of		x	
San Diego Unified Port District		x	
San Francisco, Port of	x		
Seattle, Port of			x
Shreveport-Bossier, Port of			x
South Carolina Ports Authority		x	
South Jersey Port Corporation		x	
South Louisiana, Port of		x	
St. Bernard Port, Harbor & Terminal District		x	
Stockton, Port of			x
Tacoma, Port of			x
Tampa Port Authority		x	
Toledo-Lucas County Port Authority	x		
Vancouver (WA), Port of			x
Virginia Port Authority		x	
Wilmington (DE), Port of		x	

Source: AAPA

For many of the smaller ports and some of the major ports acting as landlord ports, security within the terminals is not a major issue. Therefore, some of these ports focus only on perimeter security using government grants for this purpose. According to the results of a 1999 survey conducted by the American Association of Port Authorities (AAPA), the top 5 issues for many US and some international ports were as follows:

1. Facility expansion/modernization
2. Ability to secure funding/financing
3. Pricing pressures and new revenue sources
4. Environmental regulation
5. Railroad and highway intermodal access

Security and information technology is quite a bit lower on the list of important issues for ports (although this survey was done before September 11, 2001). Also, commercial stakeholders such as ocean carriers and shippers are not always interested in security in and of itself. If they are not being adequately compensated for spending funds to improve security, by faster service, etc, they will usually not have the incentive to do more than the bare minimum required by federal agencies. Therefore, for a port to be more willing to implement security measures and be more proactive, the measures should have both security and commercial benefits.

The security measures that were implemented range from simplistic to complex. The simple ones range from fencing, to patrol boats. Some more complex measures are

closed circuit television (CCTV) systems and x-ray or gamma-ray container content inspection. Few of the major landlord ports have already tried to implement, successfully or not, complete information tracking systems, which can result in efficiency enhancement. These information systems are described in detail in chapter 5. Most of the current and future technology measures implemented by US ports are the following:

- Fencing
- Lighting
- CCTV
- Access control
- Sonar/Radar
- Biometrics
- RFID
- Chemical and Biological Weapons Screening
- High Tech Patrol Boats
- Thermal Imaging
- Explosive Material Detection
- Radiation Screening
- Ballast Water Management
- Data Integrity
- Command Centers
- Cargo Tracking
- Security Planning/Management
- Tie-in to Federal/Local Law Enforcement

Although government agencies may be satisfied by the implementation of some these measures, most of them are not very substantive. The primary reason for this is that most of the ports lack a systems engineering approach. Most ports, especially the landlord ports, spent the available funds for the basic measures such as patrol boats, which is what funding was primarily provided for. Intrusion prevention is not the major terrorist source. If the weapon of mass destruction or hazardous chemical has already entered the port area, preventing trespassing will not do much to prevent a major disaster. Some ports for example have placed dozens of radiation detection portals (x- and gamma-ray). However, this large investment is still inadequate, since a well shielded nuclear device can easily go undetected, and having these detection portals in place can result in over-confidence, and actually result in worse results than more thorough inspection to suspicious containers. Similarly, RFID (Radio Frequency Identification), although it seems like a great technology, has some problems. The technology is not too reliable yet, and even if it were, for it to be effective, an ocean carrier would need to have all of their thousands of containers outfitted with the technology. This could be a very big investment which could possibly overshadow any benefits. I believe that more focus should be placed on detecting such threats and preventing them from entering US ports in the first place. To do this, the major ports have attempted to implement container tracking and other technologies, as part of a more comprehensive information tracking system, in order to help have more visibility throughout the shipping process and its intermodal connections.

2.3 – US FEDERAL AGENCY MEASURES

Apart from what the ports have done, federal agencies have also scaled up their operations. The US Coast Guard, Customs, INS, and others, try to ensure that vessels, workers, passengers, and cargo, comply with US laws. Also, agencies such as the TSA and the Department of Defense try to ensure that the infrastructure is safe from terrorist attacks.

Some of the important actions taken by the Coast Guard have been to conduct initial port risk assessments, redeployed assets, scaling up of surveillance of high-interest vessels, laid out groundwork for comprehensive security planning, and in general have been driving changes in security worldwide. The initial risk assessments were undertaken to identify the needs for each of the ports, and ranged from simple tasks such as the need to replace bad fencing to more complex. These assessments done by Coast Guard personnel (or their representatives) were also used to estimate the need for funding for each port. Similar vulnerability assessments were done by ports in order to identify the most common vulnerabilities and establish common standards. The redeployed vessels were Coast Guard cutters which were moved from offshore operations such as drug patrols, immigration, and fisheries monitoring, and were moved to port regions. Similarly, high-interest operations such as passenger and LNG vessels also had surveillance scaled up.

The US Customs have also stepped up their operations by inspecting containers using x-ray or gamma-ray imaging portals. However, as already mentioned, these systems are not that reliable due to the overconfidence factor. Therefore, Customs have adapted their computer systems to more effectively pin-point containers for inspection. This system was originally designed for the Customs narcotics efforts, and uses data from submitted forms to identify potential threats. This philosophy is similar to that of the information systems discussed in chapter 5. The agency has also started pre-screening cargo, by establishing operations for inspections in countries such as Canada and France.

2.4 – SECURITY SHORTCOMINGS AS IDENTIFIED BY GAO

The US Government Accountability Office (GAO) did a study on port security issues and vulnerabilities⁴. Within the fiscal year of 2004, several port-specific exercises were conducted, and coordinated by the US Coast Guard, in order to assess the response procedures that would be implemented in case of an emergency due to a terrorist attack and other such incidents. The GAO purpose for such a study was to examine (1) the emerging framework for coordinating entities involved in security responses, (2) legal and operational issues emerging from these exercises, and (3) the Coast Guard management of the analysis procedures of these exercises. 85 such tests were conducted and reviewed within the fiscal year of 2004, and four of these were observed while being conducted. The exercises conducted tackled scenarios such as the explosion of a “dirty” bomb releasing radioactive materials, approaching vessels with a bomb or hazardous chemical on board, or attacks to hinder critical intermodal infrastructure and other facilities within or around a port which would result in an economic nightmare.

The feedback from these exercises has not been very positive, which was however expected. The problems were not related to the legal authority of the federal agencies, nor were they related to statutory problems. In total there were seven legal issues that came up during the exercises. However, none of these was serious enough for any of the participants to express recommendations for statutory changes addressing these issues.

⁴ Same as note 1

The primary issues were coordination and communication problems between the authorities and other participants. Of these exercises, 59 percent resulted in feedback outlining communication issues. These issues were problems such as access to classified information when needed, inadequate information sharing across agency lines, and interoperable communication problems between first responders.

Other issues were inadequacies to coordinate resources. Of these exercises, 54 percent showed concerns with the coordination or inadequacy of resources, such as inadequate facilities and equipment. Changing levels of acceptable risk and response procedures between exercises also resulted in confusion during the exercises. The need for additional training in joint agency response seemed to be another major issue resulting in coordination problems. The feedback showed that in 41 percent of the cases there were concerns with training issues regarding the response to incident command and control environments.

Another issue, which was reported less often (28 percent of exercise responses), but is of greater importance, is a confusion about who has the authority over what. Something that is unclear among some of the agencies is what agency has the authority to raise security levels, board vessels, or detain passengers.

Besides the problems that came up from the analysis of the exercises, some of the major problems that came up were related to the response of the after-action reports by the participants, which is a common factor for most attempts to implement any new

technologies or operational procedures. These issues were primarily problems with the integrity of the reports, such as problems with timeliness, accuracy, and completeness of the responses.

The exercises that were conducted would not be of much use on their own, without sufficient feedback, and this feedback had to be timely for it to be of any use for subsequent exercises. The Coast Guard had set a deadline for the submission of the after-action reports, which was 60 days after each exercise. However, 60 percent of the responses were sent after this deadline, on average 61 days after the deadline. This greatly decreases the value of these responses, since past after-action responses were routinely reviewed when preparing for future exercises. Although participants reported that the 60 day timeline was adequate, however, most also reported that other workload kept them from meeting the deadlines. This clearly shows that since they would not be receiving any direct compensation for their time and effort of such a report, that it was set to a very low priority compared to other duties.

Besides the timeliness issue, reports were often inadequately filled out. They were asked to respond for each of the objectives of each exercise and the level to which they were met. However, 18 percent of the responses were very basic and did not have extensive feedback to assist the Coast Guard and the GAO with their assessment. The feedback lacked sufficient fundamental content, which results in a similar decrease in usefulness of the after-action response as with untimely responses. The participants,

besides having other workloads, responded that there were insufficient training and instructions for completing the after-action reports.

For the exercises to be of any use, the after-actions have to be timely and complete. Therefore, a good opportunity to improve the successfulness of the response to incidents such as terrorist attacks was lost. The Coast Guard has tried to resolve these problems by implementing new management systems to make reports timelier, and other such steps. However, these were in place for over a year without any significant improvements.

2.5 – CONCLUSION

It is clear that since 9/11 there have been many efforts by both federal agencies such as the US Coast Guard and Customs, and ports, in order to improve security measures and reduce the inherent vulnerabilities of US seaports. However, many of these efforts, although intended to be the “silver bullet” for security, have ended up being far more basic and less effective.

The primary reason behind this is the reluctance of commercial stakeholders to implement costly security measures unless it results in some form of benefit such as faster expediting of cargo, or guaranteed preference status with Customs. Ports will only spend their own funds if the measure results in better service offered, and thus more revenue. Since government funding has been limited, and in many cases only a fraction of what the Coast Guard initial estimates were, it is spent on basic improvement such as fencing (in accordance with funding guidelines).

Cooperation has shown to also be a problem for federal agencies through the GAO response alert assessment. However, in this case it is less due to inadequate incentives, but more a lack of training and knowledge of cooperating in order to establish a successful threat response system. Either way, stakeholders from both public and private parties do not seem to be very aware of the importance of everyone collaborating successfully, and seem to believe that if a few parties do not work as hard to make these

security implementations work, it will not have a big enough effect on the successfulness of the system.

CHAPTER 3 - Generic IT Needs Related to Vessel Arrival

3.1 – OCEAN DOCUMENTATION DESCRIPTION

There are several documents required by federal agencies from each vessel prior to arrival in port, as well as on entry and departure. In this chapter, these documents will be examined in order to see where possible improvements can be made.

Exhibit 3.1 is an example of the Notice of Arrival (NOA) form, required by the US Coast Guard 96 hours prior to a vessel's arrival in port. This deadline used to only be 24 hours in advance but was extended in order to give more time to federal agencies to investigate the data better and take the necessary precautions for possible threats. The key information included in the NOA is: Vessel International Maritime Organization (IMO) number, vessel name, flag, vessel owner, operator, charterer, vessel last four ports of call, ETA, destinations in the US, terminal and dock of berthing, cargo type and quantity, crew list and information, and contact phone number. Some of the data examined in order to evaluate possible threats are changes in ETA, itinerary changes, and where the crew joined the vessel. One problem area is that for the crew list page (2 of 5), no auditing for authentication is done, and the information provided is only as good as what the vessel advises.

A form required by Customs prior to arrival is Form 3171, an example of which is shown in Exhibit 3.2. The key information required is similar to that of the NOA such as vessel name and flag, ETA, owner, berthing dock or terminal, as well as some other

information such as a declaration of intentions, agency representative, manifest attachments of all foreign cargo, and the Standard Carriers Alpha Codes (SCAC) of shippers. The methods used to detect threats are the same as for the NOA.

Another document required prior to arrival in port is the original Bill of Lading (BoL). The key info requested is cargo type, description of cargo, marks and numbers, quantity, stowage, shipper, consignee, load port, BoL number, payment terms, and discharge port. One thing authorities look for are any changes on the BoL from the original.

Several other documents are required upon entry into a US port. One is the US Customs Form 1300, which is the vessel entrance or clearance statement, shown in Exhibit 3.3. The requested info for this form are the vessel particulars, IMO number, owner, operator, and vessel itinerary. Another document is the ship's stores declaration, Form 1303, shown in Exhibit 3.4. The key information included in this document is fuel amounts, stores, and bonded stores information. A problem in this document is that what is stated usually does not show what is actually on board, and the information is not examined for authentication. This is another source of potential security shortcoming. The same problem holds for the crew effects, Form 1304.

The Crew and Passenger list form I-418, shown in Exhibit 3.5, is also a document required upon entry in port, with similar problems to those of the NOA crew list section

where the information is not audited. The key information in this form is the crew or passenger's full name, date of birth, nationality, passport number, and position.

The US Customs Form 1302, the cargo declaration form shown in Exhibit 3.6, is another source of potential problems to security. Similarly to the other documents, the information is based solely on information from the vessel owner or operator, and it is not examined for inaccuracies due to the assumption that owners or operators have examined them themselves and that they have no benefit in providing the wrong information.

Another very important document is the Certificate of Origin, Form 3229, shown in Exhibit 3.8. It is a document that is used in conjunction with many other documents, such as the BoL. The manifest, Form 7512, shown in Exhibit 3.7, is another document mainly sent along with other documents, such as Form 3171.

Upon departure of a vessel, the BoL and the Customs Form 1300 have to be resubmitted. Form 1300 is the same, except that the declaration of the new cargo (1302) is attached. The BoL is also the same except for the attached Shippers Export Declaration (SED), which can also be filed electronically. For these documents, what is inspected is whether there have been any changes to the BoL or to the manifest.

EXHIBIT 3.1

Use of this format is voluntary and is intended to expedite processing of reports by the National Vessel Movement Center (NVMC).

United States Coast Guard National Vessel Movement Center		Completed worksheet may be emailed to nsme@nvmc.uscg.gov			
NOTICE OF ARRIVAL					
(33 CFR 160)					
Vessel Name	Call Sign	Vessel ID Number	Country of Registry		
PAPAYIANNIS	P8UH	8413942 <input type="radio"/> IMO <input type="radio"/> Official No.	MALTA		
Registered Owner		Operator	Classification Society		
EPAGRIS SHIPPING CO. LTD		MARINEROS COMPANIA NAVIERA SA	BV		
Name of Vessel's Charterer		Reporting Party Name	Reporting Party Telephone Number		
PAN OCEAN SHIPPING		HEATHER MOATS	(503) 228-7214		
Reporting Company		Vessel's Current Position <small>(Latitude/Longitude, place, waterway/mile marker)</small>	Date & Time of Report		
GENERAL STEAMSHIP CORP		LAT 46-33.9N LONG 154-45.8W	04/04/03 1630 HRS (LT)		
DOCUMENT OF COMPLIANCE CERTIFICATE					
Date of Issuance		Date of Expiration (if known or optional)	Issuing Agency		
05/31/00		05/24/05	BV		
SAFETY MANAGEMENT CERTIFICATE					
Date of Issuance		Date of Expiration (if known or optional)	Issuing Agency		
07/07/00		07/05/05	BV		
OPERATIONAL CONDITION OF EQUIPMENT If Not Operational, describe:					
<input checked="" type="checkbox"/> Operational <input type="checkbox"/> Not Operational <input type="checkbox"/> Not Required					
CURRENT VOYAGE INFORMATION					
Last Five Ports/Places Visited		Date of Arrival	Date of Departure		
TERNATE, INDONESIA		MAR. 14, 2003	MAR 18, 2003		
SANDAKAN, MALAYSIA		MAR. 10, 2003	MAR. 12, 2003		
TAWAU, MALAYSIA		MAR. 8, 2003	MAR. 9, 2003		
TARAKAN, INDONESIA		MAR. 6, 2003	MAR. 7, 2003		
SAMARINDA, INDONESIA		FEB. 1, 2003	MAR. 5, 2003		
U.S. Destination Port or Place/City, State		Estimated Date of Arrival at U.S. Port	Estimated Time of Arrival at U.S. Port		
VANCOUVER, WA		4/9/2003	0200 HRS (LT)		
U.S. Destination Receiving Facility/Terminal/Anchorage		Captain of the Port (COTP) Zone			
VANCOUVER, WA BERTH 9		PORTLAND, OR			
Estimated Date of Departure		Estimated Time of Departure			
04/11/03		0400 HRS LT			
Point of Contact (POC)		POC 24 Hour Telephone Number	POC Fax Number		
HEATHER MOATS		(503) 228-7214	(503) 225-9310		
General Description of Cargo		Cargo Amount	Cargo Declaration Sent to Customs? (USCS Form 1302)		
PLYWOOD AND STEEL PIPES		12535 MT	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No		
			<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		
CONSECUTIVE PORTS OF CALL					
Receiving Facility	Port or Place	City & State	24-hour POC <small>(Name & Telephone Number)</small>	Est Date & Time Arrival	Est Date & Time Departure
LAPASHA	LOS ANGELES	CALIFORNIA	GENERAL STEAMSHIP 310-380-5430	0600 HRS 04/14/03	4/16/2003

Notice of Arrival (NOA)

Vessel & Voyage Information, Version 3.0, March 20, 2003

1 of 5

EXHIBIT 3.1 (Continued)

Use of this format is voluntary and is intended to expedite processing of reports by the National Vessel Movement Center (NVMC).


	United States Coast Guard National Vessel Movement Center	Completed worksheet may be emailed to sae@nvmc.uscg.gov	
VESSEL ARRIVAL/DEPARTURE UPDATE			
Changes to NOAs must be reported as soon as practicable but no less than 24 hours (12 hours for barges) prior to entering port or place of destination. Changes to NODs must be reported prior to a vessel's departure.			
Vessel Name	Call Sign	Vessel ID Number	Country of Registry
		<input type="radio"/> IMO <input type="radio"/> Official No.	
Date of Original Report	Time of Original Report	Vessel's Original Destination	
Type(s) of Changes Included in this Report (Check All that Apply)			
<input type="checkbox"/> Destination <input type="checkbox"/> ETA <input type="checkbox"/> Voyage Info <input type="checkbox"/> ETD <input type="checkbox"/> Crew <input type="checkbox"/> Cargo <input type="checkbox"/> 24-Hour POC			
<input type="checkbox"/> Other (specify): _____			
CHANGES, ADDITIONS, OR DELETIONS			
Action	Type of Change	Change From:	Change To:
<input type="checkbox"/> Change <input type="checkbox"/> Add <input type="checkbox"/> Delete			
<input type="checkbox"/> Change <input type="checkbox"/> Add <input type="checkbox"/> Delete			
<input type="checkbox"/> Change <input type="checkbox"/> Add <input type="checkbox"/> Delete			
<input type="checkbox"/> Change <input type="checkbox"/> Add <input type="checkbox"/> Delete			
<input type="checkbox"/> Change <input type="checkbox"/> Add <input type="checkbox"/> Delete			
<input type="checkbox"/> Change <input type="checkbox"/> Add <input type="checkbox"/> Delete			
<input type="checkbox"/> Change <input type="checkbox"/> Add <input type="checkbox"/> Delete			
<input type="checkbox"/> Change <input type="checkbox"/> Add <input type="checkbox"/> Delete			
Notice of Arrival (NOA) Arrival or Departure Update, Version 3.0, March 20, 2003 5 of 5			

EXHIBIT 3.3



DEPARTMENT OF THE TREASURY
United States Customs Service

OMB No. 1515-0060

VESSEL ENTRANCE OR CLEARANCE STATEMENT

19 CFR Part 4

See back for Instructions		TRADE CODES (see back)		<input type="checkbox"/> ENTRANCE <input type="checkbox"/> CLEARANCE Check One: <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6	
1. Manifest No.	2. Port Arrival/Departure	3. Date & Time of Arrival/Departure	4. Vessel Operating Draft (in feet and inches)		
5. Nationality, Name and Type of Vessel		6. Vessel Built at/Year	7. Name, Address & Phone No. of Ship's Agent		
8. Name & Country of Owner			9. Name & Country of Operator		
10. Gross Tonnage	11. Net Tonnage	12. Port Arrived From/Departed For	13. IMO#	Official #	Call Sign
14. List All Dock Locations (continue on back if necessary)					
15. Particulars of Voyage (Previous and subsequent Ports of Call, include dates; underline where remaining cargo will be discharged.) (Con't on back)					
16. Brief Description of Cargo				17. <input type="checkbox"/> Check if Incomplete Manifest for Export <input type="checkbox"/> Check if Licensed Cargo Loaded <input type="checkbox"/> Check if Complete Manifest filed for Export	
18. No. of Crew	19. No. of Passengers	20. List All Carriers on board by SCAC Code			
21. Tonnage Mark <input type="checkbox"/> None <input type="checkbox"/> Submerged <input type="checkbox"/> Not Submerged			22. Bunkers: Type, Barrels, Value		
23. Load Line Expires	24. Solas Certificate Expires	25. Passengers Allowed Per Coast Guard Certificate	26. No. of Passengers Embarking/Disembarking		
27. Cert. Of Fin. Resp. No. (Water Pollution) and Exp. Date	28. Cert. Of Fin. Resp. (Passenger Death/Injury)	29. Cert. Of Fin. Resp. (Passenger Transportation Indemnification)			
30. PURPOSE OF ENTRANCE OR CLEARANCE <input type="checkbox"/> D (Discharge Foreign Cargo) <input type="checkbox"/> X (Export Cargo Aboard on Arrival) <input type="checkbox"/> L (Lade Cargo for Export) <input type="checkbox"/> F (FROB - Foreign Cargo to Remain on Board) <input type="checkbox"/> N (No Cargo transactions) <input type="checkbox"/> Y (Military Cargo for Discharge to be Laden)					
31. Print and Sign Name of Master, Authorized Agent or Officer, Date					
FOR CUSTOMS USE ONLY					
32. <input type="checkbox"/> Customs User Fee Paid Up*		33. <input type="checkbox"/> APHS User Fee Paid Up*		34. <input type="checkbox"/> Tonnage Tax Paid Up *	
35. Cash Receipt, CF 368 or Transaction No.		36. Total Fees Collected		37. Port Entered/Cleared, Time and Date	
38. Customs Officer Remarks					
39. Signature and Title of Officer Receiving Entry/Granting Clearance					

*Check boxes only if fees not collected

Customs Form 1300 (02/02)

EXHIBIT 3.4

DEPARTMENT OF THE TREASURY
United States Customs Service

SHIP'S STORES DECLARATION

OMB No. 1515-0059

Arrival Departure

Page No. _____

19 CFR 4.7, 4.7a, 4.81, 4.85, 4.87

1. Name of Ship		2. Port of arrival/departure	3. Date of arrival/departure
4. Nationality of ship		5. Port arrived from/Port of destination	
6. Number of persons on board	7. Period of stay	8. Place of storage	
9. Name of article	10. Quantity	11. For Official Use	

12. Date and signature by master, authorized agent or officer

This form may be printed by private parties provided they supply printed surfaces in the official form in size, wording, arrangement, and quality and color of paper.

Not required by the United States

PAPERWORK REDUCTION ACT NOTICE: This request is in accordance with the Paper Reduction Act of 1995. This information is collected to perform the responsibilities of the U.S. Customs Service. This form is used by the master to declare ship's stores in a format that can be readily audited and checked by U.S. Customs. Your response is mandatory. The estimated average burden associated with this collection of information is 15 minutes per respondent or acceptor depending on individual circumstances. Comments concerning the accuracy of this burden estimate and suggestions for reducing this burden should be directed to U.S. Customs Service, Information Services Branch, Washington, DC 20229 and to the Office of Management and Budget, Paperwork Reduction Project (1515-0059), Washington, DC 20503.

Customs Form 1303 (02/02)

EXHIBIT 3.4 (Continued)



DEPARTMENT OF THE TREASURY
 UNITED STATES CUSTOMS SERVICE
CREW'S EFFECTS DECLARATION
 19 CFR 4.7A (b) (4)

Form Approved
 O.M.B. No. 1515-0081

Page No. 1 of

1. Name of ship			2. Articles acquired abroad by officers and member of the crew (except those excluded for use on voyage or cleared through Customs authorities)			C - Cigarettes S - Spirit W - Wine
3. Nationality of ship						
4. No.	5. Family name, Given name	6. Rank or rating	C	S	W	7. No. of crewmember's declaration of articles intended to be landed (If none, show "None" opposite name)
8. Date and signature by master, authorize agent or officer						
CUSTOM FORM 1304 (111888)						

Arrival Departure

Page No.

Form Approved OMB No. 1515-0078



DEPARTMENT OF THE TREASURY
United States Customs Service

CARGO DECLARATION
19 CFR 4.7, 4.7a, 4.8, 4.33, 4.34, 4.35, 4.84, 4.85,
4.89, 4.91, 4.93, 4.96

1. Name of Ship Click in box to activate text entry		2. Port where report is made (not required in U.S.) Click			3. Nationality of Ship Click		4. Name of Master Click		5a. Port of Loading Click		5b. Port of discharge Click		Final Destination (not required in U.S.)		Date of sailing from port of loading		
Shipper(SH) Consignee(CO) Notify address (NF)		B/L No.	6. Marks & Nos. (MH) Container Nos. (CN) Seal Nos. (SH)		7. No. & Kind of Packages Description of Goods			8. Gross Wt. (lb. or kg.)		9. Measurement (per HTS)		Assess Col. 8 OR Col. 9		THIS COLUMN FOR U.S. CUSTOMS USE ONLY			
Click			Click		Click			Click		Click				Click			

See back for Paper Reduction Act Notice

Customs Form 1302 (02/02)

EXHIBIT 3.7

9-570 (1-80-108) (23-1) (23-42)

Entry No. _____

Port _____

Date _____

**TRANSPORTATION ENTRY AND MANIFEST OF
GOODS SUBJECT TO CUSTOMS INSPECTION
AND PERMIT**

U.S. CUSTOMS SERVICE

PORT CODE NO. _____ FIRST U.S. PORT OF UNLADING _____

PORT OF _____ DATE _____

O.M.B. No. 1515-0005

Entry No. _____

Class of Entry _____
(B.T.) (T.E.) (W.D.1E) (Drawback, etc.)

Entered or imported by _____ Importer/IRS # _____ to be shipped
in bond via _____ (C.I.C. number) _____ (Vessel or carrier) _____ (Car number and initial) _____ (Pier or station) _____ consigned to
Customs Port Director _____ Final foreign destination _____ (For exportations only)

Consignee _____ (At customs port of call or destination)

Foreign port of lading _____ B/L No. _____ Date of sailing _____ / _____ / _____
(Above information to be furnished only when merchandise is imported by vessel)

Imported on the _____ (Name of vessel or carrier and motive power) Flag _____ on _____ (Date imported) via _____ (Last foreign port)

Exported from _____ (Country) on _____ (Date) Goods now at _____ (Name of warehouse, station, pier, etc.)

Marks and Numbers of Packages	Description and Quantity of Merchandise Number and Kind of Packages (Describe fully as per shipping papers)	Gross Weight in Pounds	Value (Dollars only)	Rate	Duty

G.O. No. _____ Check if withdrawn for Vessel supplies (19 U.S.C. 1309)

CERTIFICATE OF LADING FOR TRANSPORTATION IN BOND AND/OR LADING FOR EXPORTATION FOR

WITH THE EXCEPTIONS NOTED ABOVE, THE WITHIN-DESCRIBED GOODS WERE:

Delivered to the Carrier named above, for delivery to the Customs Port Director at destination sealed with Customs seals Nos. _____ or the packages (were) (were not) labeled, or corded and sealed.

_____ (Inspector)
_____ (Date)

I truly declare that the statements contained herein are true and correct to the best of my knowledge and belief.

Entered or withdrawn by _____

To the Inspector: The above-described goods shall be disposed of as specified herein.

_____ For the Port Director

Received from the Port Director of the above Customs location the merchandise described in this manifest for transportation and delivery into the custody of the customs officers at the port named above, all packages in apparent good order except as noted hereon.

_____ Attorney or Agent of Carrier

Customs Form 7512 (0598)

EXHIBIT 3.7 (Continued)

INSTRUCTIONS

Consult customs officer or Part 18, Customs Regulations, for the appropriate number of copies required for entry, withdrawal, or manifest purposes.

For the purpose of transfer under the cartage or lighterage provisions of a proper bond to the place of shipment from the port of entry, extra copies bearing a stamp or notation as to their intended use may be required for local administration.

As the form is the same whether used as an entry or withdrawal or manifest, all copies may be prepared at the same time by carbon process, unless more than one vessel or vehicle is used, in which case a separate manifest must be prepared for each such vessel or vehicle.

Whenever this form is used as an entry or withdrawal, care should be taken that the kind of entry is plainly shown in the block in the upper right-hand corner of the face of the entry.

This form may be printed by private parties provided that the supply printed conforms to the official form in size, wording, arrangement, and quality and color of paper and ink. For sale by Customs Port Directors.

RECORD OF CARTAGE OR LIGHTERAGE

Delivered to Cartman or Lighterman in apparent good condition except as noted on this form

Conveyance	Quantity	Date	Delivered	Received	Received
			(Inspector)	(Cartman or Lighterman)	(Date) (Inspector)
			(Inspector)	(Cartman or Lighterman)	(Date) (Inspector)
			(Inspector)	(Cartman or Lighterman)	(Date) (Inspector)
Total					

(Warehouse proprietor)

CERTIFICATES OF TRANSFER. (If required)

I certify that within-described goods were transferred by reason of _____
to _____
on _____, at _____
and sealed with _____ or seals
Nos. _____, and that
goods were in same apparent condition as noted on
original lading except _____

I certify that within-described goods were transferred by reason of _____
to _____
on _____, at _____
and sealed with _____ or seals
Nos. _____, and that
goods were in same apparent condition as noted on
original lading except _____

INSPECTED

at _____
on _____ (Date)
and seals found _____

Inspector.

Inspector, Conductor, or Master

Inspector, Conductor, or Master

If transfer occurs within city limits of a customs port or station, customs officers must be notified to supervise transfer.

INSPECTOR'S REPORT OF DISCHARGE AT DESTINATION

Port _____, Station _____ (Date)

TO THE PORT DIRECTOR: Delivering line _____ Car No. _____ Initial _____

Arrived _____ (Date) Condition of car _____ of seals _____ of packages _____

Date of Delivery to Importer or Gen. Order	Packages	No. and Kind of Entry or General Order	Bonded Truck or Lighter No.	Conditions, Etc.

I certify above report is correct.

Inspector.

Paperwork Reduction Act Notice: The Paperwork Reduction Act of 1990 says we must tell you why we are collecting this information, how we will use it, and whether you have to give it to us. We ask for the information in order to carry out the laws and regulations administered by the U.S. Customs Service. These regulations and forms apply to carriers and brokers who are transporting merchandise in-bond from a port of importation to another Customs port prior to final release of the merchandise from Customs custody. This is governed by regulation and to your benefit.

Customs Form 7512 (0598)(Back)

DEPARTMENT OF THE TREASURY
UNITED STATES CUSTOMS SERVICE

CERTIFICATE OF ORIGIN

(ARTICLES SHIPPED FROM INSULAR POSSESSIONS, EXCEPT PUERTO RICO, TO THE UNITED STATES¹)

8. SHIPPERS EXPORT DEC. NO.		7. DATE FILED	9. CARRIER (Vessel or Airline)	9. DESTINATION (Port of)
10. CONSIGNED TO		11. LOCATION OF CONSIGNEE (City and State)		

12. MARKS AND NUMBERS	13. QUANTITY	14. DESCRIPTION OF ARTICLES	FOREIGN MATERIALS ²		MATERIALS DESCRIBED IN GENERAL NOTE 3(a)(iv)(B)(2) ³			
			15. Description	18. Value	17. Description	16. Date Imported into Insular Possession	19. Date Imported into Insular Possession	

20. INSULAR POSSESSION WHERE MERCHANDISE WAS PRODUCED OR MANUFACTURED	21. INSULAR POSSESSION OF WHICH MATERIALS ARE THE GROWTH, PRODUCT, OR MANUFACTURE
-----------------------------------------------------------------------	-----------------------------------------------------------------------------------

22. ADDRESS OF SHIPPER	I declare that I am the person named above, acting in the capacity indicated, that the description and other particulars of the merchandise specified above are correct as set forth in this certificate; that the said merchandise was produced or manufactured in the insular possession named above, and from the materials grown, produced, or manufactured in the insular possession also named above, or of the United States, or of both; that if foreign materials were used therein, their description and value are shown above. 23. SIGNATURE OF SHIPPER X
------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

VERIFICATION OF CUSTOMS OFFICER <input type="checkbox"/> I hereby certify that I have investigated the foregoing statements and am satisfied that they are correct to the best of my knowledge and belief.	24. DATE	25. SIGNATURE OF CUSTOMS OFFICER
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------	----------------------------------

3.2 – OCEAN DOCUMENTATION DESCRIPTION

It is clear that the primary concern with most of the documents each vessel needs to submit before, during or after arrival in port is data integrity. We saw the same issue arise in the previous chapter. The information is assumed accurate based on the “goodwill” of the vessel owners or operators to not send false data. This is a major source of holes in security which needs to be improved. Since federal agencies base their decision on what cargo to inspect physically from what they get out of these documents, it is a very important issue.

Another issue is efficiency. It would be very beneficial to upgrade to electronic submittals, which would be much faster to fill in as well as collect to examine. Also, if any document is accidentally inaccurate or incomplete, if it has been submitted electronically, it is easier to make the necessary corrections or additions. This way it is also easier to keep a better record of the documents for each vessel, and it is easier to compare documents before and after stay in port.

CHAPTER 4 - Following the Information Flow of an Export Container

4.1 – INTRODUCTION

The import and export process in the US is far more complicated and unique compared to most other countries. This is primarily due to sheer size, and completely different geographic attributes. With over 185 ports, and more than 100 state, local, and county agencies, navigation districts, and port authorities, the US public sector port industry is far less regulated than in other countries. Also, in the US, cargo is usually transported to the port via rail, road, or other intermodal carriers, due to the great distances where cargo often originates. In other countries however, cargo at the port originating from great distances away are actually imports from other countries, and would be considered transshipments.

This intermodal integrated system makes the US export process more vulnerable and more complicated since it adds more parties into the process. This also makes the entire data exchange process, whether hard copy or electronic, more complicated. It is therefore important to examine the information flow for the export process of a container in the US. To do this, all the stakeholders, as well as their roles and responsibilities in the process have to be identified.

4.2 – STAKEHOLDER ROLES AND RESPONSIBILITIES

A stakeholder is anyone involved in the export process of a container, including all intermodal links associated with this process, which starts from the shipper and ends at the consignee. Some of these stakeholders are common worldwide, but some are unique to the US export process. These stakeholders are not necessarily different entities. Very often, a company can have multiple responsibilities. The stakeholders in this process are:

- **Shipper/Seller:** A shipper is the individual or firm that initiates the entire process. It is the shipper's own goods that will be transported. For the tanker market, shippers are occasionally the owners or charterers of the vessels themselves. However, for containerized cargo this is not the case.
- **Freight Forwarder:** The freight forwarder has the duty to perform the tasks to assist the shipment of goods. In many countries, the freight forwarder has many more duties, which are often aligned with the duties a marine terminal operator and an ocean carrier perform in the US. A freight forwarder is hired by the shipper, occasionally along with the consignee.
- **Ocean Carrier:** The ocean carrier is the owner or operator of the vessel on which the cargo will be transported from one port to another. Some additional tasks ocean carriers perform are the coordination of the delivery of containers with the

marine terminal, maintaining an equipment inventory list (EIL), and providing a load tendering agreement for rail or truck to generate the train manifest.

- **Warehouse Operators:** They are the operators of storage areas and warehouses, and often perform tasks such as picking, packing, labeling, and sub-assembling containers. Large shippers, port or marine terminal operators, or freight forwarders are very frequently warehouse operators themselves.
- **Drayage Company:** Their task is to manage the intermodal land transportation into and out of a port (i.e. pick up and delivery) such as agreements with ocean carriers for trucking goods for intermodal transport. They often provide other various third-party logistics services.
- **Depot Operators:** Depot operators are usually located in a port, and are most commonly owned and operated by ocean carriers to own and manage containers.
- **Equipment Suppliers:** Equipment suppliers own and lease a range of intermodal equipment such as chassis, trailers, tractors, and containers.
- **Regulators:** Regulators are the government agencies that are in charge of approving and inspecting the cargo being moved, such as the US Customs, US Coast Guard, INS, etc.

- **Port/Terminal Operators:** Port operators act as mediators between the stakeholders in the loading and unloading process. Marine terminal operators typically operate for a specific ocean carrier. In the US, marine terminal operators are also in charge of clearing the cargo for Customs and other agencies. They possibly inspect containers, and must review the Drayage companies' contracts and the interchange agreements.
- **Intermodal Marketing Company:** Intermodal marketers are unique to the United States export process and work for freight forwarders and coordinate the movement of cargo between different modes.
- **Rail Carrier:** Rail carriers, as well as trucking companies and other such modes are the middle man who transport cargo from inland US to the marine terminal. They have a much larger role in the export process for the US due to the vast distances being covered, which in most countries would be considered imports and transshipments.
- **Consignee:** Consignee is the firm or individual who will eventually be the final destination of the cargo.

An illustration of how all these stakeholders of the export process interact can be seen in Figure 4.1. It is clear that the process in the US is very complicated since many stakeholders are interdependent with other stakeholders, without a clear coordinating

party in the process. In the US, the freight forwarder, ocean carrier, and terminal operators all share responsibilities such as processing the shipment, obtaining, picking, and packing containers, and preparing export documentation. On the other hand, due to the fewer intermodal stakeholders in the process, in other countries the process is far less complicated. As seen in Figure 4.2, an example of a foreign export process, the freight forwarder acts as a coordinator by collecting much more of the information that is being exchanged. At every point stakeholders send the freight forwarder updates for the freight forwarder to prepare the necessary documentations.

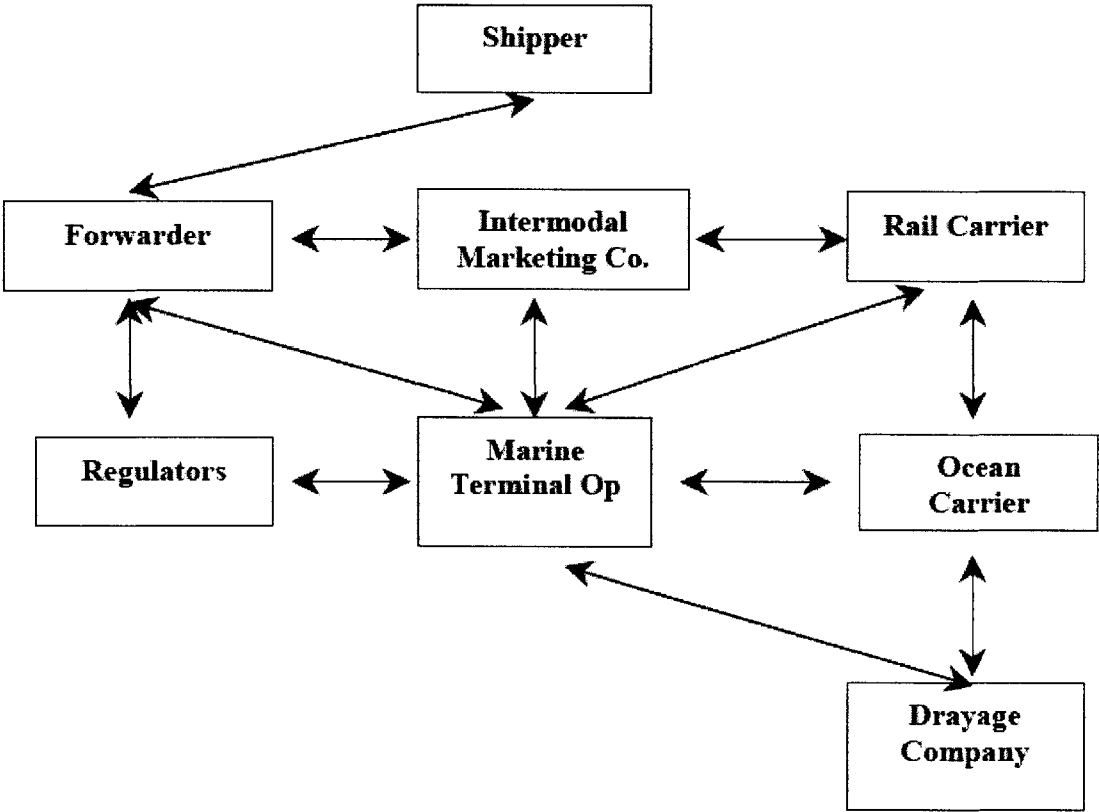


Figure 4.1: Stakeholder Interaction of export process of a container in the US
 Source: The Logistics Institute – Singapore, May 2003

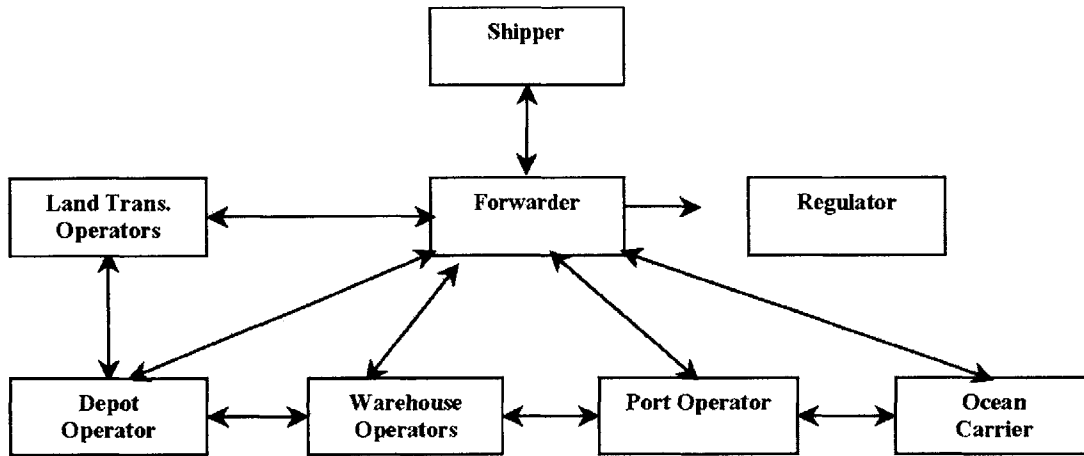


Figure 4.2: Stakeholder Interaction of export process of a container in Singapore

4.3 – CONTAINER INTERMODAL MOVEMENT

Collectively, the stakeholders have several tasks to perform in the process of exporting a container. These include (i) processing the shipment, (ii) obtaining the container, (iii) picking and packing the container, (iv) delivering the container to the port, (v) preparing export documentation, and (vi) releasing the cargo for export.

The first step is the creation of the Bill of Lading between the importer and exporter of the cargo. The Bill of Lading is used to create the Letter of Credit. The processing of the shipment is initiated by the shipper who sends the order for goods to the freight forwarder, who in turn contacts the ocean carrier to book the shipment. The freight forwarder will usually also contact the intermodal carrier who will carry out the transport through the entire supply chain from dray to rail to port.

Then, the freight forwarder will contact the marine terminal operator to produce a preliminary stow plan. The Stow Plan, along with the Carrier's Bill of Lading, Shipper's Export Declaration, and Import Berthing Application, are used to create the Export Manifest. Customs then examines the Export Manifest and decides if the ship will be cleared. The Stow plan also generates the ocean carrier Bill of Lading and the load verification.

The next step in the process to obtain the empty container. The Customer Freight Booking Request is used to create the Load Tendering Agreement for Dray and the

Booking Number. If rail is used in the process, a Load Tendering Agreement for rail is also created, which is used by the dray operator to pick up the empty container from the equipment supplier, and deliver it from one intermodal carrier to another (i.e. truck to rail, rail to truck , truck to marine terminal). Information is then sent back to the equipment inventory list, from which an EDI (Electronic Data Interchange) for the Dray Dispatch is created. The depot operators take care of the containers and swap Equipment Interchange Reports/Receipts (EIR) with the truck driver of the drayage company. The EIR is linked to the Equipment Inventory List (EIL) which is used in the cargo manifest.

Once the shipper has received the empty container and has loaded it, another EDI is created which is the Equipment Interchange Receipt (EIR) and Parking Location Assignment and are sent to the rail terminal or marine terminal for when the trucker arrives with the loaded container.

While at sea, the Ocean Carrier prepares a rail booking request EDI. An Import Berthing Application is also sent to the marine terminal prior to arrival in port. At the marine terminal, Customs may or may not inspect the container, and once they have they sent a release notice, it is then used by the Ocean Carrier to create a release notice EDI.

Once the marine terminal has received the freight release from the carrier, along with the Cargo Release from the regulatory agencies, the cargo is released to be transported out of the terminal. At this time, the marine terminal sends another Equipment Inventory Receipt for the availability of the chassis. A Load Tendering

Agreement is then sent once the container is ready to be picked up from the terminal for delivery to the final destination by truck or rail and then truck. If rail is used, another EIR is sent at the rail terminal. Once the Consignee has the cargo, the ocean carrier, drayage company, intermodal carrier, shipper/freight forwarder/shipper agent, get a paper receipt. An EIR is then sent once the empty container has been returned to the marine terminal.

The process described above is summarized in table 4.1. It is also presented as a detailed timeline in exhibit 4.1, and in the diagrams in exhibit 4.2.

Table 4.1 - Information Exchange for Export Process		
	Information Instrument	Source/Destination
1	Order for Goods	Shipper/Freight Forwarder(FF)
2	Load tendering request for Dray, Ocean or Rail	FF
3	Vessel Booking	FF/Ocean Carrier (OC) or Intermodal Marketing Company(IMC)/OC
4	Vessel Booking Confirmation	OC/FF and Marine Terminal Operator (MTO)
5	Equipment Inventory List (EIL)	OC/IMC or Equipment Supplier
6	Load Tendering Agreement	OC/Truck or Rail Carrier (RC)
7	Equipment Interchange Receipt	OC's or EC's EIL
8	Packing List	Warehouse/Dray Company (DC) and FF
9	House Bill of Lading	FF/OC
10	Ocean Bill of Lading	OC/FF
11	Export Authorization	FF/OC/Regulators
12	Cargo Manifest	FF
13	Proof of Delivery	Destination FF/ Source FF
14	Load Tendering Agreement for Dray	OC/DC
15	Trailer Interchange Agreement or Onetime Contract for Transport	OC/DC
16	Load Tendering Agreement for Rail which generates the Train Manifest	OC/RC
17	Import Berthing Application (to ensure Berth Assignment)	OC/MTO

EXHIBIT 4.1 – Timeline of data exchange for export process of a container

- **Contract for Goods, Bill of Lading/ Letter of credit:** Agreement between **Import Buyer** and **Seller**.

- **Order for Goods:** From **Seller** to **Shipper**.

- **Request for Transport with Requirements and Specifications:** From **Shipper** to **Ocean Carrier** who prepares Vessel Booking and assigns booking number. Also sent to the **Marine Terminal** by the Shipper to prepare Stow Plan, Ocean Carrier Bill of Lading, and the Export Manifest.

- **Vessel Booking Number:** sent to **Ocean Carrier's** Equipment Inventory List (EIL).

- **Load Tendering Agreement for Dray/Rail/Truck/Ocean Carriage:** Sent by Ocean Carrier to Dray Operator, Trucking/Rail company. This starts the process for pick up of empty equipment from supplier. The Load Tendering Agreement for Dray is triggered by the Ocean Carrier's EIL and sends an EDI (Electronic Data Interchange) to the drayage company and the Dray Dispatch. Load Tendering Agreement for Rail generates Train Manifest from the Rail Carrier.

- **Cargo Arrival Notification:** Sent by **Rail Carrier** to the **Ocean Carrier**. This allows driver to pick up container at the rail yard.

- **Booking Confirmation:** EDI sent by the **Ocean Carrier** to the **Marine terminal**, who requests a driver and cab. Another EDI is sent to the **EIL** once the truck had left with the empty container to pick up the cargo.

- **Equipment Interchange Receipt with Parking Location Assignment:** Requested by the terminal from the truck driver when he arrives with full container.
- **Equipment Interchange Receipt:** Sent by the Marine terminal to the Ocean Carrier once truck has arrived which triggers another EDI to the EIL.
- **Rail Booking Request:** While ship is underway, Ocean Carrier sends EDI.
- **Import Berthing Application:** sent to the Marine Terminal Operator prior to ship arrival to ensure a berthing assignment.
- **Customs Release Notice:** EDI to Ocean Carrier and Marine Terminal.
- **Freight Release:** Sent by Ocean Carrier once cargo has cleared Customs and payment has been made. This sends a message to the EIL to identify available chassis.
- **Cargo Delivery Order:** EDI sent by Ocean Carrier or customs house broker to Dray Dispatch.
- **Cargo Release:** EDI sent once the Marine terminal has received the freight order.
- **Load Tendering Agreement for Dray:** Sent by the Marine Terminal to Dray Dispatch, to ultimately result in an Equipment Interchange Receipt.
- **Delivery by Truck:** Equipment Interchange Receipt sent to Drayage company, Ocean Carrier, Intermodal Carriers once Consignee has received the cargo by truck.

- **Equipment Interchange Receipt:** Sent by the **Ocean Carrier** for the **EIL** once empty container has been returned.

EXHIBIT 4.2 – Diagrammatic representation of the Container Documentation

Exchange

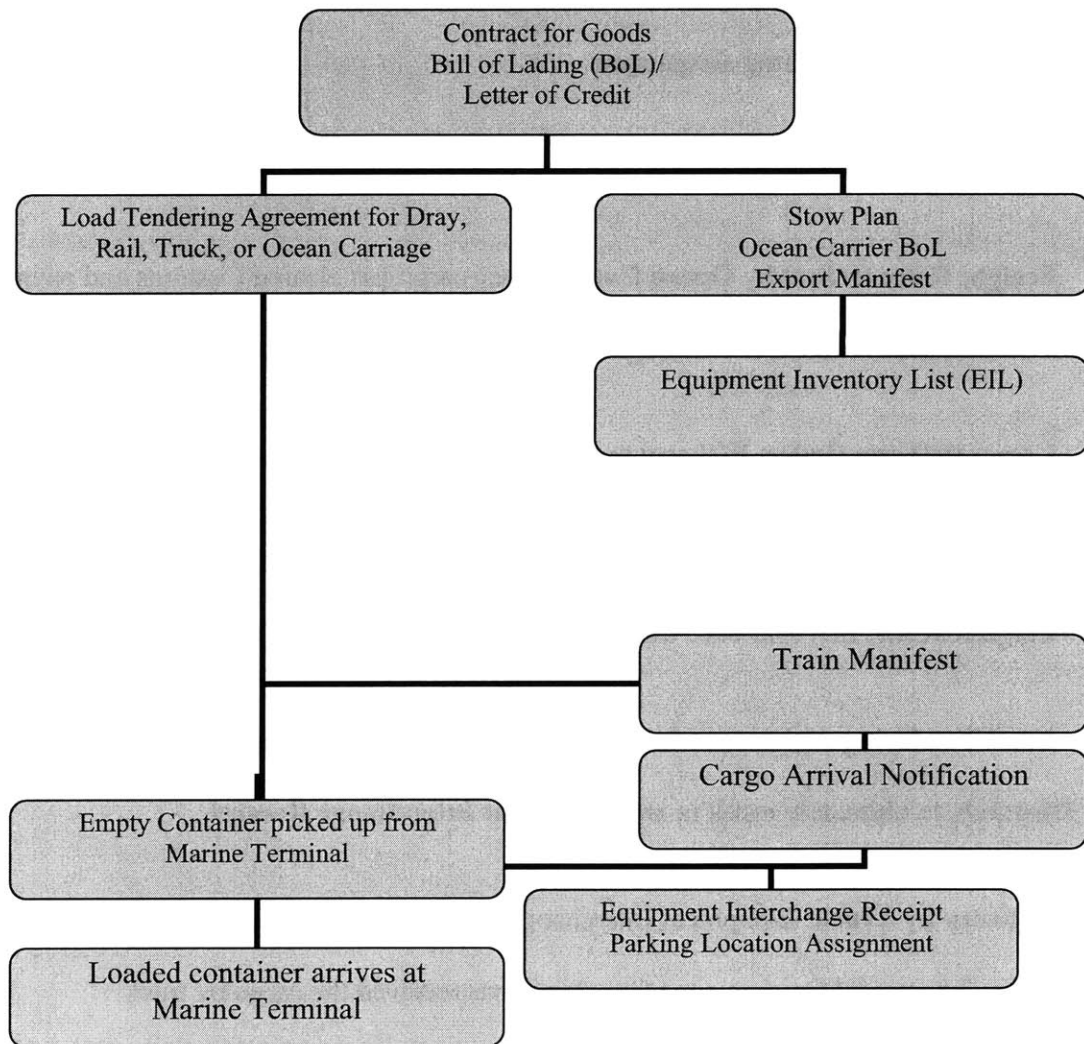
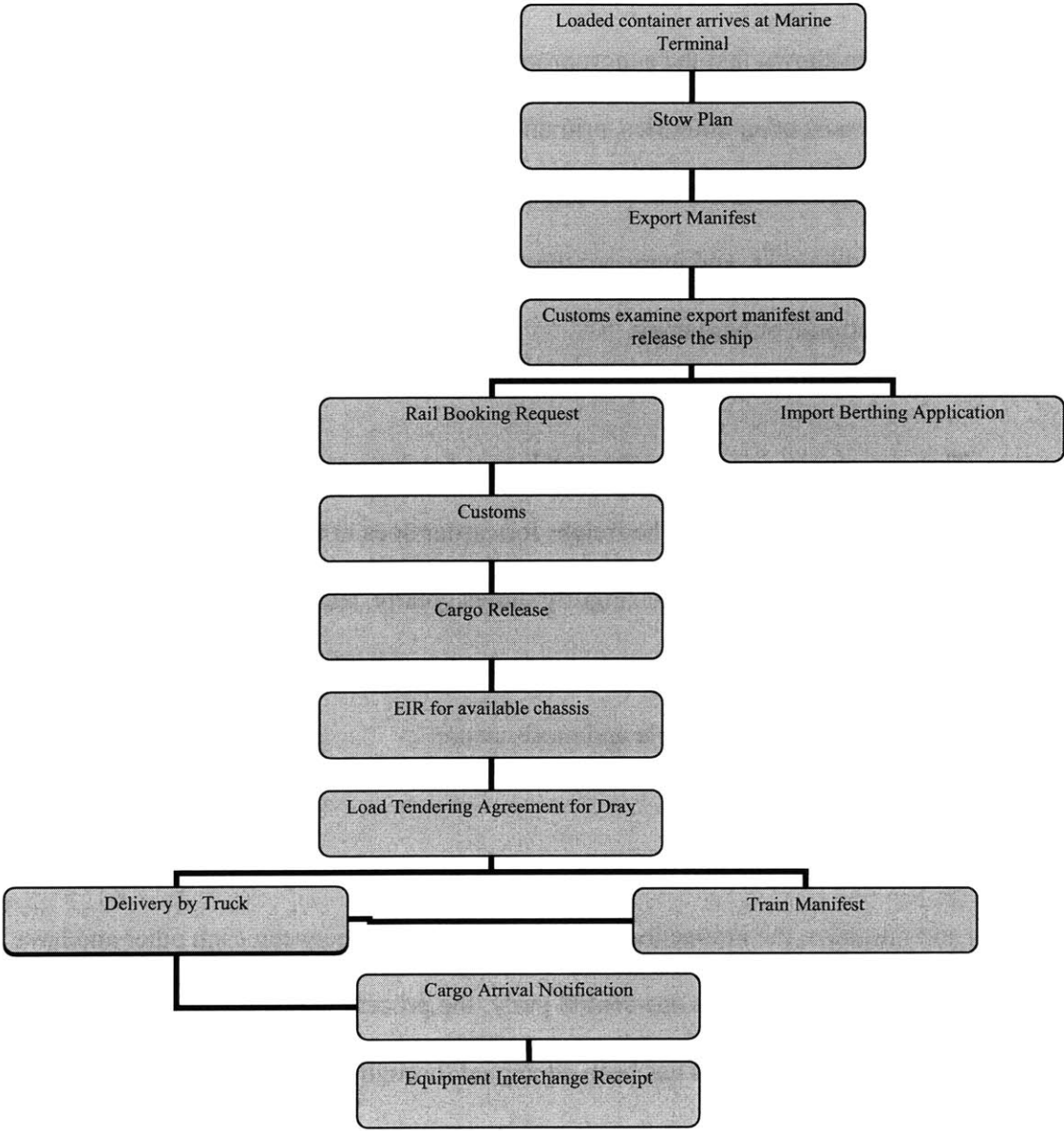


EXHIBIT 4.2 (CONTINUED)



4.4 - CONCLUSION

It has been shown that the export process of a container in the US is far more complex than in most other countries, primarily due to the vast distances covered by the cargo before it ever reaches the marine terminal. This adds more stakeholders and more steps to the whole process, and increases the amount of information being exchanged, whether it is electronic or hard copy.

This complexity is further enhanced by not having a central stakeholder coordinating everything, such as the freight forwarder does in Singapore for example. Having a coordinating party would simplify things greatly, and since someone would have most of the documents being exchanged readily available, the tracking process of the container would be more visible and more secure.

Therefore, I believe that if the US can somehow move to a more centralized process and minimize the interaction of all the stakeholders between each other and have each of them focus around that one central party, the process would become more efficient and more secure. This has been attempted through the development of “one-stop-shopping” data collecting systems which are discussed in greater length in chapter 5. Also, if more documents move from hard-copy to electronic format such as the EIR’s, the export and import processes would become even more efficient and secure.

CHAPTER 5 - Ports as Information Managers

5.1 - INTRODUCTION AND GENERAL CONCERNS

As previously discussed in chapter 2, ports are classified under two categories: landlord and operator ports. Most landlord ports, as already mentioned, have spent their budgets on Closed Circuit Television (CCTV), fencing, and other such general security measures. On the other hand, some ports in the US have taken it upon themselves to develop their own data collection systems, to enhance security and efficiency for their marine terminal and intermodal activities. Each of these systems was publicly funded to address post-9/11 maritime homeland security issues. However, these systems have failed to receive enough popularity for comparable reasons, despite their being well made technologically. Other ports have decided to simply use commercially developed software. Due to private funding rather than public funding, the focus was mostly on improving the level-of-service offered to users. Therefore, despite offering very similar features, these systems have received far wider acceptance by users from the private sector. Each of these public or private port data collecting systems are discussed in detail in this chapter.

Furthermore, companies such as Savi Technology have decided to develop specific areas in the intermodal information sector, such as electronic security seals with RFID tracking capabilities for containers. They have focused on pressuring the government for the mandatory use of this technology, which could then be incorporated in these data collecting systems.

5.2.1 - DRMEC – RISK Alert

RISK Alert is the security component of RAPID Center. RAPID is, in turn, part of the Pennsylvania non-profit organization, DRMEC (Delaware River Maritime Enterprise Council), a Pennsylvania Homeland Security national demonstration project. The budget for this project was \$1.8 million, of which \$800 thousand was a one time investment by the DRMEC for the licensing and modification of commercially available software of Transentric L.L.C., the commercial software company of Union Pacific Corporation. Initially the project received \$150 thousand from the Pennsylvania Department of Community and Economic Development (PADCED). This initial project was completed in June of 2002 by DRMEC and the Philadelphia Regional Port Authority (PRPA). It was managed for DRMEC by The Howland Group, Inc. The rest of the budget (\$850 thousand) was contributed from the \$92.3 million grant from the US Government for the improvement of port security.

RISK Alert System

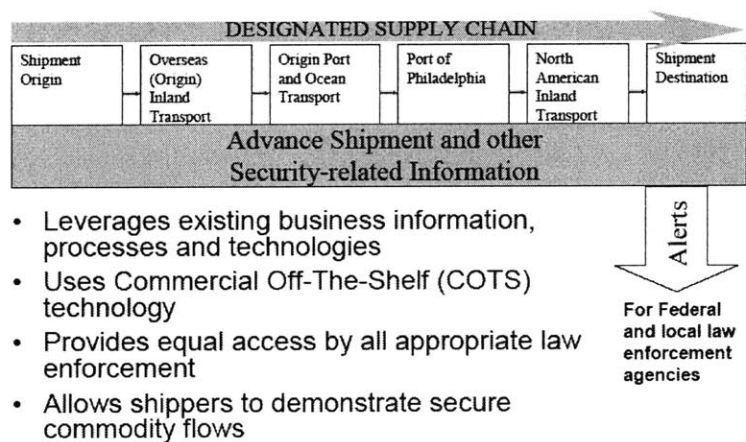


Figure 5.3: Overview of RISK Alert data flow and features

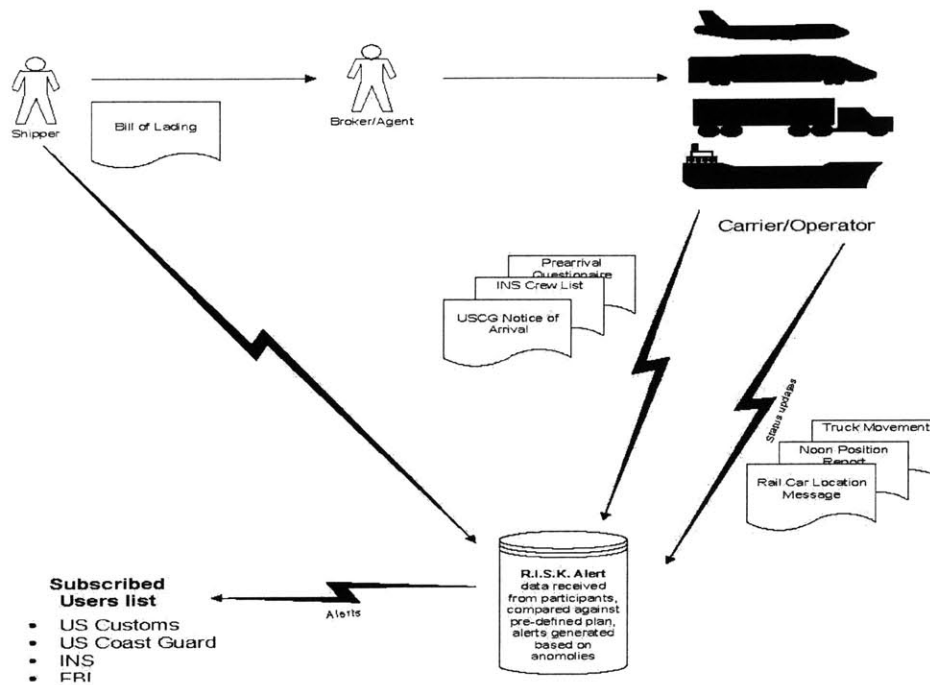


Figure 5.4: Sample of Information Flow in RISK Alert

RISK Alert was created primarily as an attempt to solve three main concerns that federal studies showed post-9/11: (1) availability to law enforcement agencies of relevant, actionable intelligence on seaport crime; (2) awareness of terrorist threats and availability of threat information to the private sector as well as to inspection personnel at seaports; and (3) integrated information on the movement of vessels, people, and cargo within seaports and ready availability of that information to government agencies and private sector security organizations. RISK Alert is a common-access transportation security information system in the country available to all levels of law enforcement. Through RISK Alert, information about shipments is available for U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, U.S. Coast Guard, and other federal and local agencies. This results in fewer delays since it allows law enforcement agencies to make informed decisions about which cargo or crew to inspect

and which to consider as secure to be expedited. The central concept was that commercial participants would “provide continually updated data about the movement of shipments through their supply chains (information which is generally maintained as a normal course of business) and law enforcement personnel would have immediate and uniform access to that data through the secure, neutral, non-profit, RISK Alert information portal. RISK Alert is also not meant to be a technology demonstration but more of an information sharing solution. It serves as a system for “one-stop shopping” information about shipments moving to or from foreign origins by ocean or land-based transport. It is also a way for shippers to show how secure their flows are to US Customs through programs such as C-TPAT. Also, unlike other similar systems that will be discussed later on, RISK Alert was not trying to be a global solution from the start, but instead started off by focusing regionally and then would try to expand as the project moves on. This would hopefully minimize some of the concerns and problems of information sharing that would likely follow.

Information on the ship’s position is captured using PoleStar’s PurpleFinder system. A screen-capture example of a PoleStar map can be seen in Figure 5.3. Apart from this, noon maritime position reports are sent daily until the ship’s arrival. It also allows for subscriptions to “alerts”, therefore customizing the information for each law enforcement representative’s separate needs. Alerts for example are sent if a ship deviates from a registered plan in such a way that should be of concern. RISK Alert also collects digital pictures, taken by the ship’s master, of each crew member, along with their names, nationalities, etc. This is done primarily to minimize confusion caused mainly by

commonalities of Middle Eastern names. This also provides added security intelligence to the local ATTF (Anti-Terrorist Task Force). Other information also submitted: Coast Guard Notice of Arrival, Coast Guard Cargo Manifest, Pre Arrival Questionnaire, and Immigrations Crew List.

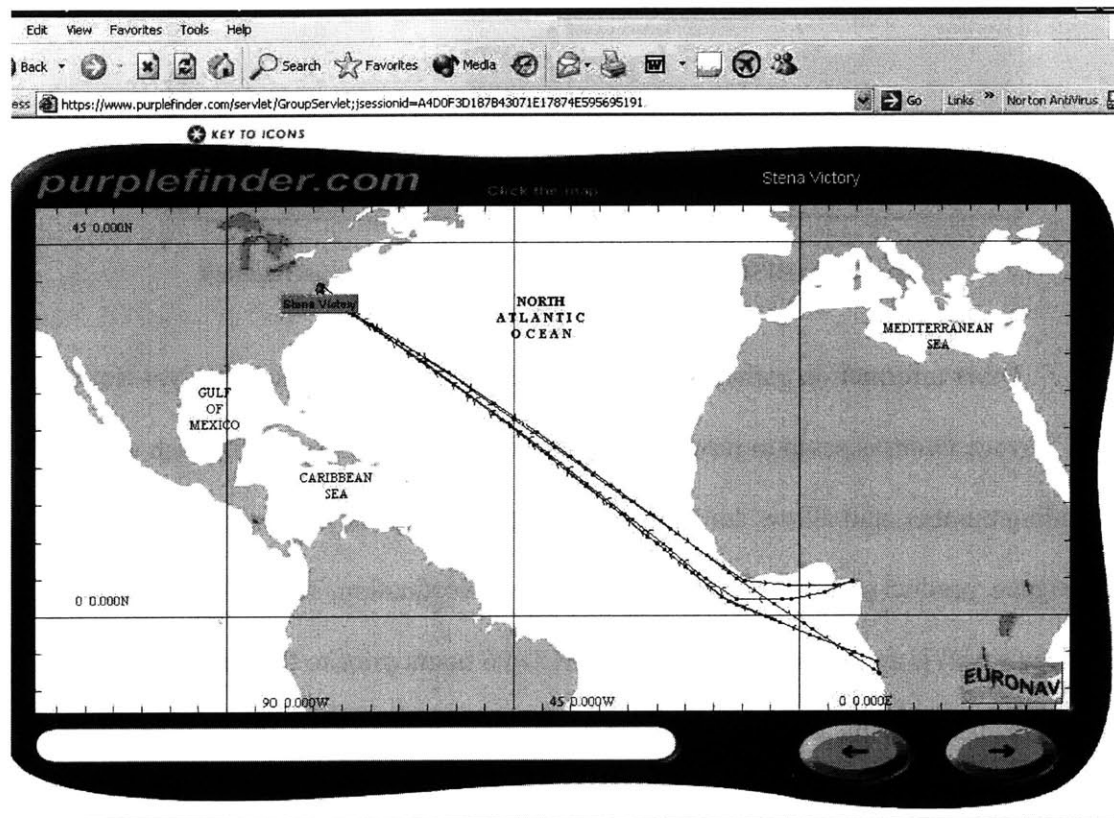


Figure 5.5: PurpleFinder screenshot

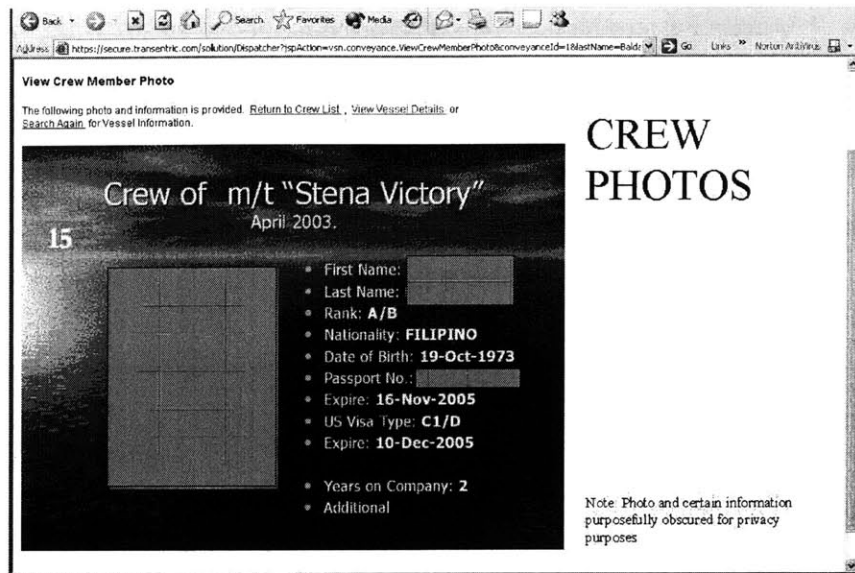


Figure 5.6: RISK Alert crewmember information page screenshot

Other information gathered is the Voyage Order and the Vessel Arrival Notice. The Voyage Order is setup to receive basic information about shipments, such as the bill of lading number, and allows someone to uniquely identify the shipment, shipper, consignee, product and quantity, and the origin and destination. The Vessel Arrival Notice (VAN) is a document used by the USCG 96 hours prior to the vessels arrival into port. This includes the Vessel Automated Manifest System (AMS), which is an electronic cargo declaration. The VAN includes a notice of vessel arrival, and a Pre-arrival questionnaire, which is also used to possibly generate alerts. It also includes an INS form which contains crew information.

5.2.2 PROOF OF CONCEPT DEMONSTRATION

A national proof-of-concept demonstration of the capabilities of RISK Alert started on January 27th 2003. The purpose of this demonstration was to train and present RISK Alert features to law enforcement agencies and government personnel. This demonstration, however, although initially planned to track containerized meat shipments from Australia, was instead performed with two VLCCs (Very Large Crude Carriers) operating between West Africa and the Delaware River, with the cooperation of the Sunoco, Inc. oil company. Since DRMEC was interested in making RISK Alert a national standard for improving efficiency and homeland security, they would have to expand beyond containers, which are however the most complicated. In addition, the Delaware River supported the largest petrochemical refining center on the East Coast, adding to DRMEC's interest in this sector. Therefore, by using tankers, DRMEC was simplifying the tracking process by minimizing the information needed, and also was able to show that their system can be implemented for the entire shipping community, and not just containers. Although this demonstration was able to demonstrate RISK Alert abilities to successfully deliver information to law enforcement agencies, the information being shared was too small to provide sufficient proof that it could function as an effective deconfliction tool and as a tool to bring the large number of stakeholders together.

In general, the demonstration resulted in positive feedback from the participants. This encouraged DRMEC to propose that the USCG adopt RISK Alert as a standard maritime homeland security system. This proposal was rejected, along with similar

proposals from other systems, showing that the business of maritime homeland security is not yet mature enough to yield a standard system for incorporation into federal law.

Despite the positive feedback, many concerns were put forth as recommendations for future changes to the system. The main challenge, as expected, was ensuring the sufficient cooperation and coordination between stakeholders. As indicated earlier in this chapter, this has been the main focal point for all of these “one-stop” systems being developed. For commercial stakeholders, the main concern was the involuntary release of confidential records such as trade secrets or proprietary information, due to gaps in security, especially since the data would be shared on the internet. Something like that could damage a firm’s reputation, lower consumer confidence, and result in a decrease in market share, without sufficient incentives and returns from the existence and use of systems such as RISK Alert. There are also many issues arising from the need for these systems to get data from government agencies on potential threats, in order to be able to react to potential vulnerabilities more effectively. One concern is national security, which may prevent agencies from sharing information. If information is to be shared, declassifying it can take too long and would no longer be of any use to time-sensitive operations. The other concern is that people who need access to this information may not have the security clearances necessary.

All these concerns have led to similar problems to those outlined by GAO and presented in chapter 2. It is not a surprise that the initial survey responses after the demonstration yielded positive remarks. With the small amount of data, it was a

relatively easy task to manage the data timeliness and accuracy and completeness, and therefore the majority of the data received was timely.

Although in the majority of the cases the Voyage Order was received two weeks before the vessel's departure, despite the limited participants, there were still cases where this information was only received a day prior to departure or not at all. The fact that the demonstration participants voluntarily agreed to take part in this demonstration but still had some trouble with sending information on time makes this problem even bigger. This would only expand very rapidly to a major concern when the entire regional shipping community is involved in this process.

In some cases, the Voyage Order, besides not being in sent on time, was incomplete. For example, the name of the vessel was missing. In some other instances, the shipment number was incorrect. Although DRMEC support that this was not a problem since by contacting the shipping agents they were able to obtain the information they needed, this would only work for the limited data being exchanged in the proof-of-concept demonstration. It is highly unlikely that DRMEC would have the resources to successfully manage to retrieve missing information from many more shipping agents, and more importantly to actually manage to do so on time for the information to be of any value at all.

There are many other instances of data integrity issues besides the Voyage Orders. One example is instances of inaccurate or missing crew member date-of-births on

INS documents and crewmember pictures. Another example is inaccurate Noon Position Reports. In one instance, the noon report sent one day was identical to the one sent the previous day, although the ship was not stationary. More important than any of these issues were inaccuracies observed on the VAN, a far more critical element to RISK Alert. In some cases, information of the next port of call and date of call were missing from the VAN. More troubling is that the information on the VAN and other documents rarely was verified for authenticity. It was simply assumed that the data provider had already verified the data authenticity.

Moving beyond the data integrity issues, during the demonstration there were many other problems with the system. First of all, the data was input manually, which is less accurate and far less efficient. This was acknowledged by DRMEC as a feature that needed to be changed for use beyond the pilot demonstration. Besides this improvement, DRMEC had in plan to possibly include a vessel maintenance history and vessel stowage plan in the data collected. Also, it was requested that passport country and number be added to the crewmember information. A more complicated improvement requested was the improvement of the loading of the shipment plan. For the pilot, RISK Alert shipment plan was created and loaded into RISK Alert manually, which would be impossible to do when this has to be done for thousands of shipment plans considering how labor intensive this process is. Therefore, in order for RISK Alert to be function, this feature has to be automated first.

RISK Alert funding has been discontinued, and the project has been put on the shelf. The data integrity issues led commercial stake holders to be doubtful about the system. Commercial participants did not seem to be getting enough in return. The risk of proprietary information leaking out to competitors was too large.

5.3.1 PORT OF NY/NJ – F.I.R.S.T.

The Port Authority of New York/New Jersey (PANY/NJ), supported by the Federal Highway Administration Office (FHWA), has developed a “one-stop shopping” system for cargo information tracking similar to RISK Alert; the Freight Information Real-Time System for Transport (FIRST). One main difference from RISK Alert is that its primary focus was not security, but instead congestion mitigation. The FIRST project was initiated before the 9/11 crisis, which could be one of the main reasons behind some of the most important problems FIRST was facing. Post 9/11 funding was drastically reduced, especially for the purposes of marketing and reaching out to the port community. It also resulted in the project being rushed, and the focus being shifted midway into the development of the project.

Americas Systems, Inc (ASI) designed and maintained the website and server, and also processed the data flow. Unlike RISK Alert which was based on off-the-shelf commercial software, FIRST was designed from scratch by members of the private sector intermodal industry in cooperation with public sector partners. FIRST used File Transfer Protocol (FTP), and collected information from ocean carriers, terminal operators, and rail and trucking companies. FTP was used to encourage data providers to provide their data to FIRST, since charges from using Electronic Data Interchange (EDI) would be eliminated. The main issues FIRST was trying to address were reduction of truck queue lines by reducing the number of necessary trips by trucks to the port, and thus ultimately

reduce emissions, as well as improving terminal operation efficiency and at the Port of NY/NJ overall.

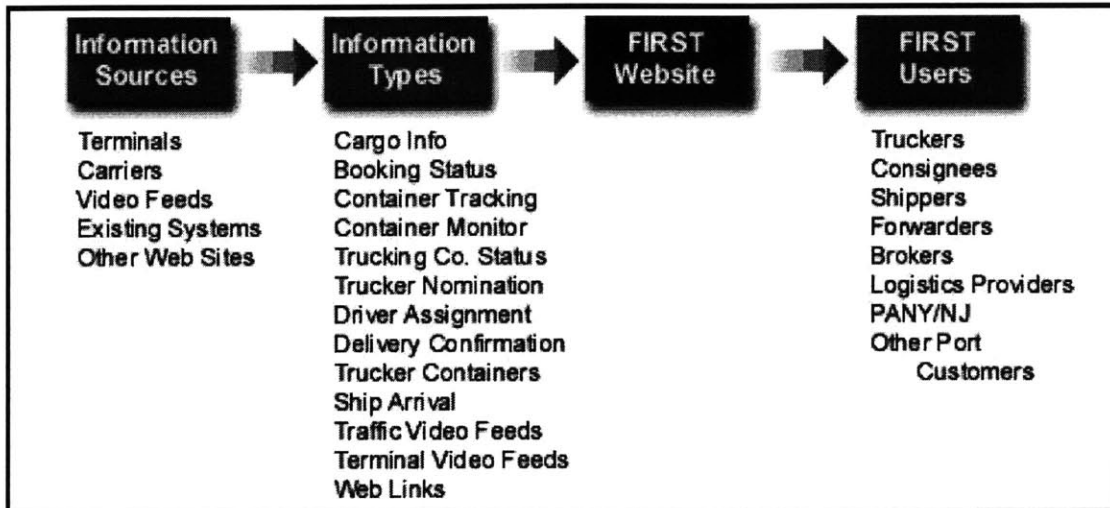


Figure 5.7: FIRST Information sources, types, and users

The main feature that FIRST offers is real-time information on cargo status, including customs status, hazardous cargo information, vessel or carrier, date in, etc. They also provide real-time booking status, container tracking of all movements for the past 90 days, including container monitoring with alerts for pick-up, gate transactions, inspections, weights, destination and proof of delivery. It also offers vessel schedules, web cameras, and port traffic conditions. A useful feature on the FIRST web-site is the ability to create, view, and edit a watch-list of containers that are of interest. It was also planned to incorporate into FIRST the Coast Guard's Vessel Traffic Service (VTS) and the Customs Automated Manifest System. VTS are shore-side systems which range from simple information messages to ships, such as position of other traffic or meteorological warnings, to management of traffic within a port or waterway. Ships entering a VTS area report to the authorities by radio, and may be tracked by the VTS control centre.

FIRST successfully integrated SEA LINK, a trucker identification system. SEA LINK eliminates most of the paperwork a truck driver has to present when entering a marine terminal for pick up and delivery, reducing delays. It provides computerized registrations for a trucking company's drivers, allowing truck drivers to pick up and deliver cargo to and from any terminal they have authorized access to using a single ID card.

Another feature planned was Cargo*Mate, a chassis tracking system for the FIRST system, to provide end-to-end cargo visibility. It uses RFID and GPS technology to track a chassis' location, size/type, history, tether status, in/out facility information, container association, and even its tire pressure, cargo weight, mechanical condition, and inspection status. For this it utilizes built in sensors, microprocessors, modem, GPS, and a rechargeable battery. Table 5.1 shows how these features are available to different levels of access to the FIRST system.

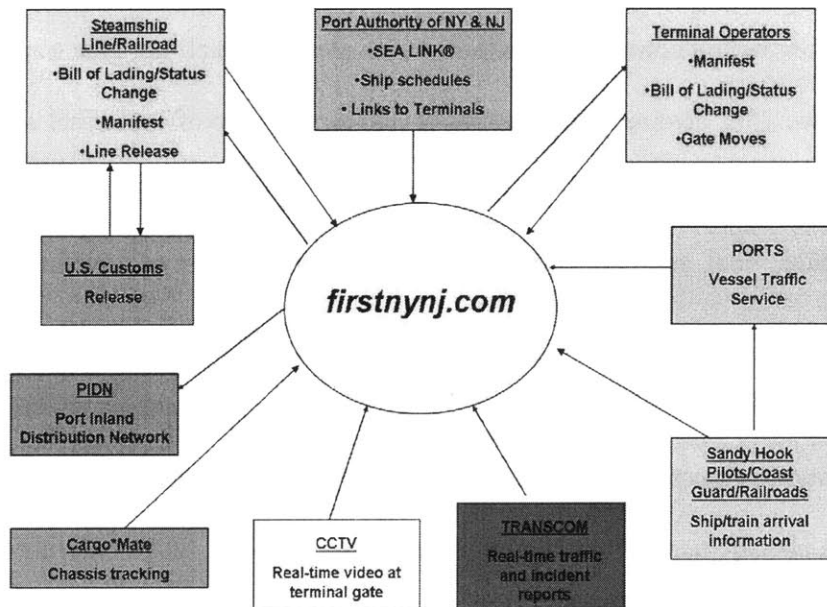


Figure 5.8: Overview of FIRST

Table 5.1 - Levels of Access to FIRST System Features

Feature	Public Access	Basic Registered User Access	Specific/ Special Business Access
Container Trace	•	•	•
Booking Inquiry	•	•	•
Port Traffic Alerts	•	•	•
Port Directory (including SEA LINK® Inquiry)	•	•	•
Vessel Activity Inquiry	•	•	•
Waterway Activity	•	•	•
Web Cameras (PNCT, Global, Interport Gates)	•	•	•
Watchlist Menu (monitor, create, edit)		•	•
USDA Search		•	•
Cargo*Mate® Chassis Search		•	•
Truck Nominations			•
Truck Appointment System (FUTURE)			•
U.S. Coast Guard Vessel Traffic Service (FUTURE)			•
Customs Border Patrol Automated Manifest System (FUTURE)			•

5.3.2 CONCERNS

Although FIRST was technologically successful, it did not catch on as much as expected. In order for FIRST to be fully functional, it is required that the information be received from all terminal operators and shipping lines servicing the Port of NY/NJ. This became increasingly more difficult, which has resulted in FIRST only using the site for the online berth application function from the beginning of 2005. The participants did not feel they were getting enough in return for providing all this information for free.

Terminal operators are asked to answer additional inquiries from trucking companies,

which causes additional work. Truckers are also required to visit multiple websites to collect all the needed information, also resulting in extra work.

There were good signs of interest with almost 4500 monthly hits on the website just after its launch in 2001. This was mainly triggered due to increased demand due to 9/11. However, the hits dropped to around 1000 by early 2003. The container tracking feature usage also decreased from 1000 to 100 monthly hits. Registration was also very limited to make FIRST a viable solution. Only around one percent of motor carriers in the Port of NY/NJ had registered by 2003.

Similar to the main problem that RISK Alert was facing, FIRST had problems ensuring the integrity of the data being transferred on their site. Registered users often found that information was missing, late, or inaccurate. Ocean carriers and terminal operators have the responsibility over the accuracy and timeliness of the data they send, and although FIRST allows them to do so at no cost via FTP, they did not have any incentives to guarantee data accuracy. On many occasions, ocean carriers and terminal operators would have received several data updates when only one set of data had been posted on FIRST. Just like with RISK Alert, ocean carriers were hesitant to share all their information due to the risk of proprietary information leaking out due to gaps in security on the website. This was only further enhanced by the purchasing of ASI by Maersk Data, which created a serious conflict of interest. In addition, the limited funding which would stop by the end of 2003, meant that FIRST does not have the technical staff required to successfully address data quality issues.

Providing FIRST services at no cost has also been a major reason for the system not being accepted more widely. Although this was initially thought to attract more attention from participants, it meant that once funding was stopped in December 2003 that the available features would depreciate without revenues to support their operation. For FIRST to continue, new forms of funding would have to be found. One possibility would be to provide a fee based service, with different fees for different levels of services. This lack of funding resulted in another issue as well. Since it was greatly limited due to post-9/11 measures, it resulted in FIRST being introduced with fewer features, with a plan to add the rest as the project progressed. However, a move like that was detrimental, since without the full features upfront, such as the truck appointment system, the benefits such as decreased congestion were not apparent. If FIRST had the proper funding and had introduced a stronger product from the start, the results would have been more apparent to the system's potential users, who would have been keener to subscribing and continuing the use of FIRST services.

The FIRST system failed to solve any of the issues initially centered on. Since it was never widely accepted by the private sector, and ocean carriers and marine terminals were not very willing to provide their information, they failed at improving efficiency by reducing the time trucks spent in queues to enter a terminal, and the number of unnecessary trips taken by truck drivers. This meant that the issue of reducing emissions was also not resolved.

5.4.1 EMODAL

Another “one-stop shopping” information system that has been developed is eModal. Unlike RISK Alert and FIRST, eModal is a private, for-profit company portal, providing their services for a fee that changes depending on the level of usage. The project was initiated in Irvine, California in 1999, and the website was up and running by February of 2000. The other two systems were focused on one specific port and region, and had plans to expand if the project succeeded. On the other hand, eModal started as a system targeted to multiple ports. It has grown to be the most widely used system in the US port community with 14 ports and 36 terminals supplying information to their database, and over 6400 registered users by 2003. eModal started with similar objectives to those of the FIRST system, such as improving efficiency and decreasing congestion at container terminal. This is primarily since both were initiated prior to 9/11. Therefore, their main focus was not port security. Unlike FIRST that had the pressure to adapt to the new demand for security and change their scope, eModal, as a private company, remained focused on efficiency rather than security.

The features being offered on eModal are similar to those offered by FIRST, such as weather conditions at terminals and ports, FTP data transmissions to minimize costs, real-time cargo information, container tracking and monitoring, and trucker nominations. It does not offer any real-time booking information at this time. eModal does not offer chassis tracking such as the FIRST system’s Cargo*Mate, nor does it provide real-time traffic information. However, it is the only system with a feature that allows the payment

of demurrage and other such fees online. It is also unique by offering the Electronic Delivery Order (eDO) system. The eDO system is a feature that allows registered users to receive, track, and manage delivery orders electronically, which is an efficiency enhancing tool.

5.4.2 CONCERNS

Although what eModal offers is technologically very similar to what FIRST had to offer, it managed to get far wider acceptance in the industry than FIRST ever did. To emphasize this even more, the main focus of the FIRST system, the Howland Hook marine terminal in the Port of NY/NJ, is now using eModal. They had the luxury of not having to change their focus towards security issues. Since they had launched prior to 9/11, they did not have to rush to launch their system. FIRST was greatly affected by post-9/11 demand for security, and was therefore not able to do careful business planning like eModal did. Despite the fact that FIRST was free, eModal came up with a fee based structure that was accepted by its users. Since eModal was not receiving government funding, and was charging its users for the services, it was more focused on meeting user needs on time and cost benefits rather than satisfying government needs for maritime homeland security. This is precisely the reason eModal has been so widely accepted. The success of these “one-stop” information systems is highly dependent on the acceptance by users in the private sector, who are primarily concerned on reducing their costs and improving efficiency, which is not something that FIRST or RISK Alert focused on.

5.5.1 INTERNATIONAL SYSTEMS - PORTNET

The Port of Singapore (PSA), with over 9.9 million TEUs handled in the first half of 2004, is the world's leading port in the handling of containerized cargo, and has not stayed behind in the recent efforts to introduce efficiency enhancing IT services as part of the services they offer. They have been offering IT services since 1984. PSA has developed the PORTNET system, which was launched on May 8th, 2000, and encapsulates 16 years of experience. Besides the port-wide solution, PSA has also developed CITOS for marine terminal-specific use.

Similarly to eModal, PORTNET is not focused around post-9/11 maritime homeland security needs, but rather solely focused on efficiency for shippers and ocean carriers. With the immense volume of containers handled daily by PSA, PORTNET was slowly becoming a necessity in order for Singapore to remain competitive and offer high levels of service. Without this efficiency enhancing system, service would deteriorate as volumes keep growing, and shippers and ocean carriers would slowly seek new less congested ports.

PORTNET has proven to be a rather successful system, and therefore PSA has decided to offer this system as a package to other ports, similar to what eModal is doing. One port in the United States that showed interest for the package was the Port of Seattle. In January of 2001, they signed a Memorandum of Understanding with PSA, to market,

implement and operate a Web-based information technology system for the Port of Seattle.

PORTNET users can make use of online ordering and documentation, and track and trace capabilities such as real-time booking status, vessel tracking, and container tracking via their Cargo2D2 feature. The PORTNET system brings together shipping lines, freight forwarders, shippers and government agencies, and facilitates business-to-business transactions for the port and shipping industries. PORTNET also enhances productivity and reduces operational costs for users through efficient information management through its database.

5.6.1 SAVI – SMART CONTAINERS

Apart from complete IT intermodal solutions such as those presented above, there have been developments in more specific areas of the intermodal system. One of the most prominent developments has been RFID tags for containers, such as “Smart Box” containers, with Savi Technology being the leader behind the efforts of establishing this technology. Electronic seals on containers can also be used for the tracking features in the aforementioned “one-stop” data systems.

Savi has been working hard with the US Department of Homeland Security (DHS) and the Customs and Border Protection (CBP) for the development of the Customs Trade Partnership Against Terrorism (C-TPAT), and is seeking the adoption of its ‘Smart Box’ technology as a US standard. C-TPAT is an initiative that hopes to get shippers to become more proactive on security issues by providing better service in return, such as “green lane” qualification. The most secure shippers with “green lane” or even the new level of “bright green lane” qualification would get preferable treatment such as immediate cargo release without inspection.

Features included in ‘Smart Box’ RFID tags include the ability to automatically detect intrusions, sense interior environmental changes in temperature, humidity, tilt, light, shock, vibration, and atmospheric pressure, and the ability to detect hazardous cargo such as radioactive materials and wirelessly communicate their location and security status to a global information network in real-time. The door-end of a container

is fitted with multiple sensors, Electronic Product Code (EPC)-compliant smart tags and active radio frequency identification (RFID) technologies.

As outlined by Savi, the potential benefits of using 'Smart Box' technology for shippers are reduced inventory, reduced out-of-stock, reduced lead-time variance, increased manufacturing uptime, reduced administrative costs and fees, theft prevention, and the prevention of lost containers. Such benefits, along with green lane clearances, can help in attracting shippers and ocean carriers, since as mentioned before they are hesitant to freely improve their security standards without sufficient incentives in return.

Although the 'Smart Box' technology is a very good concept for both government agencies and commercial stakeholders, I believe adopting the technology of a single provider such as Savi should be avoided, especially since Savi is a for-profit organization. However, promoting the high-tech container seal technology as a whole, and incorporating it by making it compulsory in the near future, could be beneficial if it is reliable and cost effective.

5.7 CONCLUSIONS

In this chapter, many intermodal data collection systems for the use of ports and marine terminals were presented in detail. All of these systems, whether they were developed by a collaboration of government authorities and specific port authorities, or by private companies developing their own software, had very similar technological features. They all provided methods to track container movements and their booking status in real-time, as well as other real-time cargo data. They also offered features such as vessel tracking and trucking nominations. To differentiate from each other, they all offer unique features, such as the FIRST system's Cargo*Mate chassis tracking, and eModal's eDO system. However, none of these features alone was enough to explain the reason behind the success of one system over another. From a technology standpoint, all the systems presented in this chapter were well designed solutions.

A common concern between RISK Alert and FIRST, and possibly the most important reason for their limited success, was their primary focus: maritime homeland security. Although this scope satisfied the needs put forth by several agencies, it did not satisfy user needs. Users, such as shippers, ocean carriers, freight forwarders, rail and trucking companies, and terminal operators were not as concerned with homeland security as much as with efficiency of operations and cost reduction. Users did not see enough of a return on investment for spending the time to send accurate and timely information to these systems' databases. This resulted in a cyclical problem, since with

these data accuracy, timeliness, and completeness issues, the level-of-service also drastically deteriorated, and the primary goals were not resolved.

Apart from the data accuracy issues, there are also other integrity issues. Private users feel that there is a great risk that proprietary information can fall into competitors' hands, which can result in enormous losses. Although this should have been a problem for the private systems as well, it did not seem to be part of the user mindset. This is most probably due to the general satisfaction of users due to the many efficiency-enhancing and cost reducing benefits they were receiving, which could overshadow the data security issues. In addition, the private systems typically did not ask for company-sensitive information.

Another issue faced by RISK Alert and FIRST, which is related to their focus on homeland security, has to do with funding, and pressures to develop the systems as soon as possible. Since they were relying on limited government funding which was eventually split between all major US gateways, and needed to show results quickly, they did not spend nearly as much time and money as necessary on marketing the products successfully. One mistake was to start offering incomplete services with the intent to develop the rest and include them at a future date. This way, the benefits were not as apparent to the early users. Therefore, they were hesitant to further utilize the systems.

In order for these operator ports to successfully develop “one-stop shopping” information solutions, they have to focus around the needs of all the potential users/stakeholders, rather than simply satisfying government agency perceived needs.

CHAPTER 6 – Conclusions and Recommendations

The focus of this thesis was on an approach taken by some ports to collect and manage large amounts of cargo movement-related data (A separate approach would be to communicate specific pieces of this data rather than to collect and manage it; please refer to the thesis by Alexander Sichel on *Supply Chain Security and Information Technology* for further information on this approach).

Summarizing the conclusions of the previous chapters, we have seen that ports have been reluctant in spending any substantial amount of their own funds on improving security measures beyond the minimum requirement by governmental authorities. This has been primarily because ports are not convinced that if some of these measures are implemented in certain ways, along with other changes in operations, they could be offering better and more efficient services to carriers and shippers. The government has tried to promote improvements with the C-TPAT initiative and Safe and Secure Trade Lanes, such as the “green lane”.

Some of the ports that have realized this, however, have gone beyond the basic security measures and have taken a more proactive role in their operation practices, and have decided to do more about data collection and tracking. Even in this case, however, the pressure the government has been putting on these one-stop-shopping systems to be developed quickly and with limited funding due to the 9/11 crisis, has resulted in these systems focusing on the wrong issues (from the perspective of providing a service that

stakeholders will pay for). They have focused on the security benefits, rather than on creating efficiency and cost benefits for all stakeholders which would in turn result in security enhancements.

A recurrent issue that has been found in each of the chapters concerning different types of information being exchanged between stakeholders is the issue of data integrity. GAO outlined problems on timeliness and completeness, even from government agencies. Many documents that have to be prepared prior to a ship's arrival are also dependent on the "goodwill" of commercial parties to provide accurate data, which is not always the case. RISK Alert and FIRST have both had problems with ensuring that their participants cooperate and send in the information needed. In these cases, if every participant does not do his part properly and completely, the entire system ceases to work properly. RISK Alert and FIRST have both shown that commercial stakeholders have limited incentives to spend time and money on sending information that could damage their entire business if it managed to leak out to the wrong hands. On the other hand, eModal has focused on efficiency of operations since they did not have pressures from the government and are a private firm. It seems that in some cases the government, by trying to implement measures as soon as possible, managed to worsen the problem by preventing the development of viable solutions.

Another major problem that has been shown in this paper is the many stakeholders in the export and import process due to the large intermodal network creating added complexities. The problem is that too many stakeholders have many

responsibilities, without a central coordinating member. This causes many inefficiencies in the process, and also makes the tracking process of potential threats all the more difficult. Data integrity issues are a problem in this case too, and because of this dispersion of responsibilities and lack of a coordinating member, it is especially difficult and unnecessarily time consuming to track where the inaccuracy originated from in order to pin point the threat and prevent it on time.

Judging from the success of eModal and PORTNET, that were dedicated to improving efficiency of the cargo flow, it is clear that similar future systems, or current systems being revised and enhanced, should follow the same pattern. Security improvements are bound to follow if all the participants in the system have a good incentive to send timely and accurate data resulting in a better database. Federal agencies should take this into account and not put as much pressure on the swift development of programs that will only be shelved at the end. Rushing to fix the security shortcomings that have existed for so long will not help. It is better to come up with a more thought out and comprehensive solution and have the risk of problems continuing in the short run while it is being designed and see very good long term results, than to come up with a solution as soon as possible and end up having it not be as effective as possible in the long term.

However, collecting data for these systems would be much simpler and faster if there was a central coordinating member in the process of exporting or importing a container, since fewer stakeholders would have to bother with spending time and money

on this, making the benefits clearer. The ideal would be to give more responsibilities to a particular party, such as freight forwarders in the example of Singapore, and have information be sent back to them. This way the majority of information these systems would come from one party and would be easier to manage and check for inaccuracies. The IT systems that have been developed such as RISK Alert would have similar effects. However, most of the systems have proven not to work due to commercial participant unwillingness to fully participate and share their information. However, if these data systems are designed to simply collect the information that is already exchanged between stakeholders and shown in chapter 3, the potential results may not be as good, but they may be far more feasible.

I also believe that US federal agencies should continue with initiatives such as Safe and Secure Trade Lanes and the “green lane”, etc. However, they have to make sure that when they are offering preferential treatment through fewer customs inspections, that they actually deliver what they say. A major rule in marketing is that any marketing technique can only be successful as long as the product it is marketing lives up to the promises being made. Up to now, the benefits have not been too visible, and commercial participants are being discouraged from following these initiatives. The problem may also be originating from the fact that these programs are at their infancy, and as they grow, their benefits become clearer. Also, in the future, the government should examine the funding related to the maritime supply chain, and should focus on improvements that help prevent possible threats from ever entering the ports rather than keeping trespassers out of the areas.

GLOSSARY OF TERMS AND ABBREVIATIONS

09/11	Refers to the terrorist attacks on the US in 2001
AAPA	American Association of Port Authorities
AMS	Automated Manifest System: electronic cargo declaration
ASI	Americas Systems, Inc: designed and maintained the RISK Alert website
ATTF	Anti-Terrorist Task Force
Biometrics	Electronic ID cards for port workers
BoL	Bill of Lading: document required prior to arrival in port
Cargo*Mate	A container chassis tracking system for the FIRST system
CCTV	Closed Circuit Television: monitoring system for port security
Consignee	The buyer of the cargo
C-TPAT	Customs Trade Partnership Against Terrorism
DRMEC	Delaware River Maritime Enterprise Council
EDI	Electronic Data Interchange
eDO	Electronic Delivery Order: feature of eModal that allows registered users to receive, track, and manage delivery orders electronically
EIL	Electronic Inventory List
EIR	Electronic Interchange Reports
eModal	Data management system developed by private firm
EPC	Electronic Product Code
FHWA	Federal Highway Administration
FTP	File Transfer Protocol

GAO	US Government Accountability Office
GPS	Global Positioning System
IMO	International Maritime Organization
INS	US Immigration and Naturalization Services
Intermodal transportation	The transportation of containers on two or more modes (ship, rail, truck, barge, air)
IT	Information Technology
Landlord port	A port that is not involved in the actual Terminal operations
LNG	Liquefied natural gas
NOA	Notice of Arrival: see VAN
Noon Position Report	Requirement of RISK Alert to provide information daily on a vessel's position
Ocean Carrier	A company that owns and operates ships
OPA 90	Oil Pollution Act of 1990, in the US, requiring double- hull configuration for oil tankers
Operator port	A port taking an active role in operations within the Terminal
PADCED	Pennsylvania Department of Community and Economic Development
PANY/NJ	Port Authority of New York and New Jersey
PORTNET	Data management system developed by PSA
PRPA	Philadelphia Regional Port Authority
PSA	Singapore Port Authority
RFID	Radio Frequency Identification
RISK Alert	All-in-one data collection system by DRMEC

Savi	Logistics company providing military and commercial users with container tracking and securing technology
SCAC	Standard Carriers Alpha Codes: a unique two-to-four-letter code used to identify transportation companies
SEA LINK	Trucker identification system used in FIRST system
Shipper	The firm sending/selling the cargo
Smart Box	Container with RFID technology developed by Savi
TEU	Twenty-foot equivalent unit: a standard for measuring container capacity
TSA	Transportation Security Administration
U.S. Customs and Border Protection (CBP)	A government organization that maintains control over the importation and exportation of goods into the US
US Coast Guard	A government organization that, in part, enforces the marine safety regulations of the US
US DHS	Department of Homeland Security
VAN	Vessel Arrival Notice: a document used by the USCG 96 hours prior to the vessel's arrival into port
VLCC	Very Large Crude Carrier
Voyage Order	Is setup to receive basic information about shipments, such as the bill of lading number, and allows someone to uniquely identify the shipment, shipper, consignee, product and quantity, and the origin and destination
VTS	Vessel Traffic Services are shore-side systems which range from simple information messages to ships, such as position of other traffic or meteorological warnings, to management of traffic within a port or waterway

BIBLIOGRAPHY

1. The Logistics Institute — Asia Pacific, *Comparison of Singapore and USA Sea Cargo Container Export Processes*. Erera, Kwek, Goswami, White, Zhang, May 2003
2. US Department of Transportation – Federal Highway Administration Operations Unit, *Freight Information Real-Time System for Transport Evaluation Final Report*. J. Srour, J. Kennedy, M. Jensen, C. Mitchell, October 2003.
3. Booz-Allen, *Intermodal Process Map*. May 2000.
4. US General Accounting Office, *Nation Faces Formidable Challenges in Making New Initiatives Successful*. JayEtta Z. Hecker, August 2002
5. US General Accounting Office, *Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention*. January 2005.
6. Delaware River Maritime Enterprise Council, *RISK Alert National Proof-of-Concept Demonstration Final Report*. September 2003.
7. Southern Methodist University, *Systems Engineering Approach to Analysis of the United States Critical Infrastructure and US Ports as Subsystems of the Extended Enterprise System*. Susan Vandiver, 2004
8. Volpe National Transportation Systems Center, *Innovative ITS Technologies with Joint Security and Mobility Benefits*. Joseph S. Koziol, Jr, April 2004
9. US Department of Homeland Security, *Secure Seas, Open Ports*. June 2004
10. Containerization International, *C-TPAT Gets Bright Green Lane*. March 2005
11. Containerization International, *DHS Seals its Security Needs*. March 2005
12. American Journal of Transportation, *'Smart Box' Technology Goes Beyond US Customs*. February 2005.
13. eModal website: www.emodal.com
14. Port of Seattle website, www.portseattle.org, Port Signs MOU With Singapore's Portnet.com. January 2001.
15. Singapore's (PSA) PORTNET system website: www.portnet.com
16. RISK Alert website: www.riskalert.org