MARITIME SUPPLY CHAIN SECURITY:
Navigating through a sea of compliance requirements

EMMA MASPERO
ESBETH VAN DYK
HANS ITTMANN
hittmann@csir.co.za
Logistics and Quantitative Methods
CSIR Built Environment

ABSTRACT

As a direct result of the 9-11 New York attack all modes of freight and passenger transportation were scrutinised for vulnerabilities. Over 90% of international trade takes place via sea transport for at least some part of the supply chain and as a result there has been a drive to better secure maritime transportation. This paper outlines the background to and the rationale behind the most important of the new security measures for maritime transportation and provides an overview of the likely implications for supply chain role-players. In addition the paper endeavours to create awareness of the importance of maritime supply chain security.

TABLE OF ACROMYMS

Acronyms	
AMR	Advanced Manifest Rule
CBP	Customs and Border Protection
CSI	Container Security Inititiative
C-TPAT	Customs and Trade Partnership Against Terrorism
DHS	Department of Homeland Security
JIT	Just-In-Time
IMB	International Maritime Bureau
IMO	International Maritime Organisation
ISPS	International Ship and Ports Facilities Security Code
IT	Information Technology
MTSA	Maritime Transportation Security Act
RFID	Radio Frequency Identification
SAFE	Security and Accountability For Every port
SOLAS	Safety Of Life At Sea
SST	Smart and Secure Tradelane
UNCTAD	United Nations Conference on Trade and Development
US	United States of America

INTRODUCTION

Most supply chain security initiatives are driven by the United States of America (USA) in direct response to the shortcomings revealed in freight and passenger transportation security post 9-11. As over 90% of international trade takes place via sea transport for at least some of the supply chain, there has been an understandable drive to better secure maritime transportation (wwwa). However, given the sheer volume of programmes/initiatives and new policies it can be difficult to navigate a clear path through the sea of acronyms let alone achieve full compliance. This paper outlines the background to and the rationale behind the most important of the new supply chain security measures and provides an overview of the likely implications for supply chain role-players.

BACKGROUND TO SECURITY INITIATIVES

On 11 September 2001, the face of transportation was changed forever in the terrorist attacks on the Twin Towers in New York using passenger airplanes. As a direct result of the 9-11 New York attack, and the subsequent scrutiny of all modes of transportation for vulnerabilities, the IMO (International Maritime Organisation – a United Nations body) recognized the need for increased security within maritime shipping and so the SOLAS (the Safety of Lives at Sea) Convention Chapter 11 was amended to provide for the inclusion of the International Ships and Port Facilities Security Code (ISPS Code), which was internationally adopted in July 2004. This initiative was quickly followed by a spate of other measures and programmes introduced by various authorities aimed at addressing different facets of securing the international maritime supply chain. One of the overriding challenges has been to formulate and introduce measures that provide for increased security without hampering or interrupting the smooth flow of goods.

As so much freight is transported by ocean, any large-scale attack on a seaport (or even major shipping line's vessel) is almost guaranteed to have far reaching ripple effects into the global economy at large. While it is almost impossible to quantify the exact contribution to the economy by shipping, the United Nations Conference on Trade and Development (UNCTAD) estimates that the operation of merchant ships contributes approximately US$380 billion in freight rates within the global economy, which is roughly equivalent to some 5% of total world trade. Shipping trade estimates are most usually calculated in tonne-miles (i.e. tonnes carried multiplied by the distance travelled.) In 2003 alone, the maritime shipping industry moved approximately 6.1 thousand million tonnes over a distance of some 4 million miles thus resulting in the rather staggering total of over 25 thousand billion tonne-miles of trade being facilitated. This trade volume is increasing steadily. It is estimated that within the last four decades, seaborne trade traffic has more than quadrupled. (wwwa)

Since the adoption of the ISPS code, other transportation security measures/ initiatives have been introduced aimed at increasing preparedness and vigilance to promote and ensure safety of goods and people engaged in international trade

through sea ports. All of these measures have a cost (financial, human and system) and, where in the economics of international trade the cost/benefit trade-off is carefully weighed and balanced, so to, must the costs of these initiatives be taken into account. *"Measures taken by the US and other governments to improve homeland defense have burdened the global transportation system, creating longer and less reliable lead times."* (Sheffi, 2001)

But how exactly does one go about securing a supply chain? Is it even possible to secure and account for an entire international network of transportation modes spanning the globe (often more than once), involving a multitude of role-players all operating to different standards and with very different risk profiles, and if it is possible to secure the entire chain, how can it be done in a cost effective, efficient manner that does not interrupt the physical flow of goods?

OVERVIEW OF INITIATIVES

A multitude of initiatives and programmes have been introduced to secure various aspects of the maritime supply chain. Maritime and port security measures are not and should not only be aimed at addressing and combating the risk of terrorism but also other threats such as piracy, and smuggling. Piracy is on the increase and is of particular concern to maritime operations in certain "hot zones" in Indonesia, Malaysia, the Indian subcontinent and along the Eastern Coast of Africa (wwwb). South African ports, on the other hand, face a relatively low risk of international terrorist attack, but high incidences of illegal human movements through stowaways and trafficking as well as smuggling of illegal substances.

Although much has been written about the various security initiatives, only two articles were found that give a brief overview of a number of the most important initiatives (Flynn, 2006; wwwc). Two further reports were found that provide an in-depth overview of the security initiatives around the world (National Board of Trade, 2008: SIRPRO, 2008). The key elements of the most relevant of these initiatives to South African industry and maritime role-players are described in more detail below:

Initiative 1: The International Ship and Ports Facility Code (ISPS)

The Safety Of Life At Sea Convention (SOLAS) was amended to include a new appendix, namely the International Ship and Port facility Security Code hereafter referred to as the ISPS Code. According to the International Maritime Organisation (IMO), there are currently 148 contracting governments and some 9600 registered port facilities world wide, 57 of them in South Africa (wwwd).

The ISPS Code is a fairly simple two-part policy that:

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

The ISPS code requires ship and port facility staff to:

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

The ISPS code addresses all aspects of maritime shipping through code adherence by the major parties involved:

- the vessel
- the vessel owner (shipping line)
- the port
- port facilities (terminals and operations at the port)

Compliance to Part A of the ISPS code is mandatory and covers:

- responsibilities of contracting governments
- declaration of security
- obligations of the company

- ship/port security assessments
- ship/port security plans
- ship/port/company security officer assignment and responsibilities
- training and drills
- survey and certification

Compliance to Part B of the ISPS code is not mandatory for Contracting Governments; rather it focuses on fleshing out Part A and provides numerous examples for the adoption of, compliance to and adherence to Part A. Most of the IMO member countries have however treated part B of the code as mandatory.

The IMO is not a statutory body and therefore cannot enforce compliance to the ISPS code. However, through member nations indicating compliance (which for many countries was at the time an “intent to comply” rather than actual compliance due to the vast scope of the code), the onus was transferred to contracting governments to draft suitable national legislation within which the compliance to the ISPS code would be housed.

In December 2002, when the ISPS code was launched, contracting governments were set a deadline of 1 July 2004 for compliance. Many countries felt sure that due to the severity of the ISPS code requirements and the implications for international trade, the deadline would be extended or even that the requirements of the ISPS code would be relaxed. Instead neither happened and many developing nations have struggled to comply to the requirements lacking the financial, human and technical resources necessary to achieve proper compliance. A major shortcoming of the ISPS code to date has been the widely different interpretations of the requirements contained in the code and the lack of standardised auditing of compliance by a neutral international body.

Initiative 2: Container Security Initiative (CSI)

Parallel to the ISPS Code development, the US Customs and Border Protection (CBP), began developing anti-terrorism programs to help secure the United States in direct response to the 9-11 attacks. The CSI targets international movement of

containers for closer scrutiny. Containers are vulnerable to terrorism as almost any commodity can be transported in them legally and illegally (such as stowaways, dirty bombs and other weapons.)

According to CBP[1], the core aims of CSI are to:

- identify high-risk containers
- pre-screen and evaluate containers before they are shipped
- use technology to prescreen high-risk containers (includes large-scale X-ray and gamma ray machines and radiation detection devices)
- use smarter, more secure containers

As stated in the factsheet published by CBP (wwwe):
"The primary purpose of CSI is to protect the global trading system and the trade lanes between CSI ports and the US. Under the CSI program, a team of officers is deployed to work with host nation counterparts to target all containers that pose a potential threat."

According to the CSI 2006 – 2011 Strategic Plan, CSI is currently operational in the following ports (wwwf):

CSI compliance ports world-wide	
The Americas:	**Middle and Far East:**
■ Montreal, Vancouver and Halifax, Canada	■ Singapore
■ Santos, Brazil	■ Yokohama, Tokyo, Nagoya and Kobe, Japan
■ Buenos Aires, Argentina	■ Hong Kong
■ Puerto Cortes, Honduras	■ Pusan, South Korea
Europe:	■ Port Klang and Tanjung Pelepas, Malaysia
■ Rotterdam, The Netherlands	■ Laem Chabang, Thailand
■ Bremerhaven and Hamburg, Germany	■ Shenzhen and Shanghai
■ Antwerp and Zeebrugge, Belgium	■ Kaohsiung
■ Le Havre and Marseille, France	■ Colombo, Sri Lanka
■ Gothenburg, Sweden	■ Dubai, United Arab Emirates (UAE)
■ La Spezia, Genoa, Naples, Gioia Tauro and Livorno, Italy	■ Mina Raysut, Oman
■ Felixstowe, Liverpool, Thamesport, Tilbury and Southampton, United Kingdom	**Africa:**
■ Piraeus, Greece	■ Durban, South Africa

■ Algeciras, Spain	
■ Lisbon, Portugal	
■ Zeebrugge, Belgium	

It is clear from the above table that it is operational primarily in countries with which America has favourable trade and diplomatic relationships, which are, by their inclusion in the programme, the countries that would be expected to pose the smallest risk for harbouring terrorism. For CSI to be truly effective it should ideally be extended to high risk countries such as: Afghanistan, Iran, Iraq, the Baltic states, etc. although this would be very difficult to implement. However, promoters of CSI are quick to point out that CSI is designed to provide the most "bang for the buck", in that approximately 60% of containerised cargo entering the US is sent from a CSI compliant port (wwwg). One of the principles of CSI is to screen the highest volume of containers with scarce resources.

Initiative 3: Customs-Trade Partnership Against Terrorism (C-TPAT)

C-TPAT is a voluntary membership based programme aimed at increased security through partnership between US customs and supply chain role-players such as importers, customs brokers, terminal and warehouse operators, transporters and foreign manufacturers and focuses on increased information exchange to improve overall supply chain visibility. Described by Robert Bonner (Commissioner of Customs and Border Protection), the guiding principles of C-TPAT are voluntary participation and jointly developed security criteria, best practices and implementation procedures. In exchange for increasing security of their own and partners' operations within the supply chain, members enjoy expedited handling and inspections of their products by US Customs. According to the 2007 cost-benefit study undertaken, the primary motivations to join the programme are: *"For all businesses, 'reducing the time and cost of getting cargo released by CBP' is the most important potential benefit, followed by 'reduced time and cost in CBP secondary cargo inspection lines'… According to Importers, the most important motivation for them to join C-TPAT is to "to reduce the disruptions to the supply chain". For non-importers, 62% indicated that their principle (sic) reason for joining the program was that their business partners required them to be C-TPAT certified."* (Diop, Hartman & Rexrode, 2007) While C-TPAT is a membership by invitation programme and has been restricted to role-players in the US, Canada and Mexico,

the programme is gradually being extended further afield and the first steps to formally include Chinese role-players have been taken (wwwh).

The principle of C-TPAT is imminently sound; through extending port borders outwards and into industry, better security is achieved as well as improved supply chain visibility which is in line with international best practice. In criticism it must be recognised that the initiative promises expedited handling in exchange for membership. One possible unintended consequence of broadened membership (best represented by the forthcoming roll-out to China) could be that growing membership may exceed the program's carrying capacity and end up slowing, rather than facilitating and speeding the process.

Initiative 4: Advanced Manifest Rule (AMR)

The US Customs and Border Protection Agency (CBP) instituted an Advanced Manifest Rule (AMR) in February 2003, whereby detailed cargo data must be submitted to US Customs at least 24 hours prior to lifting containers onto a vessel bound for an American port. The premise behind AMR is that containers will only be allowed into America if detailed contents information has been provided electronically to Customs at least 24 hours before the container is loaded on the ship. The information will be used to pre-screen containers prior to arrival in the American port and to select questionable containers for physical inspection. Besides US ports requesting AMR, the World Customs Organization (WCO) in Brussels has also been developing standard sets of customs data elements and guidelines for member countries to enable advanced electronic transmission of such data (Lee, 2004).

Initiative 5: Better packaging

The challenge is not only to secure the ports and vessels themselves against attack or theft but also to improve security of the product's own shipping packaging. With the continued increase in the use of containerised shipping, the focus has been extended beyond scanning of containers as outlined in the CSI programme to developing technology to better seal and monitor containers in transit. Both initiatives outlined below were introduced to pioneer and pilot the use of "smart boxes" and seals on containers, all of which strive to reduce container tampering or unauthorised opening:

- **Operation Safe Commerce**

Launched in 2002 as a programme to fund business initiatives designed to enhance security for container cargo moving throughout the international transportation system (wwwi).

- **Smart and Secure Tradelane initiative**

On July 2, 2003, the Smart and Secure Tradelane initiative (SST) was announced whereby the world's three largest seaport (and terminal) operators – Hutchison-Whampoa Ltd, PSA Corporation Ltd. and P&O Ports, which together represent more than 70% of the world's container traffic, would collaborate to demonstrate and deploy automated tracking and security technology for containers entering US ports through the use of seals on the containers to prevent tampering (Lee, 2004).

It is important to note though that while these initiatives are necessary and valuable first steps, to truly secure any supply chain, an integrated approach is required. The mechanics of supply chain security combine physical security and IT security elements with a process orientation for decision making (Emigh, 2005).

REPERCUSSIONS OF THE IMPLEMENTATION OF THE VARIOUS INITIATIVES

The primary concern regarding the implementation of increased security measures must be the disparity of resources available within, and to, maritime nations to achieve compliance. The US has created enabling legislation in the form of the Maritime Transportation Security Act of 2002 and the subsequent Security and Accountability For Every Port (SAFE) Act of 2006, both of which provide for substantial resources to be allocated to increased border protection and security. In particular the SAFE Port Act authorizes $400 million to be made available in annual federal port security grant funding for five years from 2006 (wwwj). Over the four years prior to 2006, it is estimated that $708 million was allocated for maritime security. This amount was highly criticised by US port operators and authorities who claimed it was approximately 20% of what the port authorities had identified as needed to properly secure the ports. In contrast, South Africa has spent some R220 million on improved security; largely to improve physical security such as fences and

some technology in the form of new cameras (Van der Merwe, 2006). Many developing countries simply lack the financial, technical and human resources necessary to properly secure their maritime ports. As a result, they face blacklisting by international bodies such as ISPS or being bypassed by shipping lines in favour of more secure ports. *"At the time of implementation, South Africa had few port officials with the necessary expertise and experience to lead an immense security overhaul. Planners were largely creating security procedures and organisations from the ground up without adequate international guidance. Officials stressed that it was especially difficult for developing countries to marshal the economic resources and manpower required to achieve international compliance. They suggested that international assistance with training and funding would make developing nations much more likely to comply with international standards."* (Lyndon B. Johnson School of Public Affairs, 2006)

Another concern regarding the implementation of increased maritime security measures is the wide range of different interpretations of the regulations. This was clearly illustrated in the LBJ research project which conducted surveys in seven countries revealing inconsistencies in the interpretations of the ISPS Code when during visits to each country, *"it became clear just how inconsistent ISPS is from port to port and country to country. While the language of ISPS is uniform in each port and in each country, it was as if we were seeing seven different codes…. The inconsistencies in implementation methods from country to country as well as differing opinions on ISPS, serve to reiterate the importance of harmonization and international standards. Our research highlights many of the financial and ideological discrepancies in different countries that must be taken into consideration when developing and trying to implement such globally significant legislation."* (Lyndon B. Johnson School of Public Affairs, 2006)

A positive outcome of the implementation of new security measures has been the accompanying increase in research on supply chain security: MIT researchers at the Centre for Transportation and Logistics (CTL) conducted studies to understand how supply chains are impacted by disruptions such as terrorist attacks, natural disasters and other logistics failures (wwwk). Researchers at Stanford have published a recent white paper on supply chain security (wwwl), while private sector firms such as IBM

(wwwm) and APL (wwwn) also conducted research on the subject. A recent Lloyd's Practical Shipping Guide examines the cost of security to port terminals and the implications to industries while highlighting the shift from terminal security to supply chain security. The Guide also proposes various risk assessment models (Bichou, Bell & Evans, 2007).

IMPLICATIONS FOR THE GLOBAL SUPPLY CHAIN

The requirements for compliance with the various initiatives can be stringent, and in addition to the resources required to ensure proper integration of compliance with day to day operations (as discussed above), there are also far-reaching general supply chain implications. The primary implications are:

Implication 1: Know your partners

Supply chain experts seem torn between whether it is best for a firm to have one or two suppliers or a range of suppliers to reduce the "hold-up problem" and diversify risk. When supply chain security is considered, the debate is weighed very much towards a small number of trusted suppliers with whom the firm is very familiar, and whom the firm can partner with in reducing risk through increased visibility and information sharing.

Implication 2: Re-evaluate stock-keeping strategies

In the immediate aftermath of 9-11, many US companies took active steps to move from Just-In-Time (JIT) to more of a Just-In-Case stock keeping philosophy whereby some companies began ordering parts from overseas suppliers in larger quantities and increasing safety stocks to keep their assembly lines moving "just-in-case" their inbound transportation was disrupted. In addition, they planned to keep more finished goods on hand so customers can be supplied even when the manufacturing process is disrupted, (Sheffi, 2001). This presents the supply chain with a new twist on an old dilemma: how best to ensure that integrity of the supply chain is maintained while not incurring unnecessary inventory holding costs or recreating the bullwhip effect of amplified stock-keeping that was one of the main reasons most role-players embraced JIT as a way of guarding against overstocking. The private sector (particularly American role-players) have also experienced the cost of heightened

security in the form of overall reduced supply chain confidence. Freight and insurance rates rose steeply in the year following the 9-11 attack and some companies expanded their supply bases and investigated sourcing from local suppliers (even at a higher cost) in an attempt to safeguard against potential international transportation disruptions (Lee, 2004).

Implication 3: Invest in supply chain visibility tools and technology

As a result of increased supply chain initiatives, industry role-players are having to provide more information than ever before to authorities regarding the exact whereabouts of cargo and who has had direct physical contact with that cargo. To this end, *"by and large, corporate customers want supply chain security technology that will let them comply with government requests for information sharing, while at the same time protecting product data from their competitors."* (Emigh, 2005) Therefore the use of technology such as RFID (radio-frequency identification) and GPS to monitor, track and trace cargo is becoming more widespread and is no longer restricted to high-value cargo.

RFID technology can be used to track the movements of containers and as such has been heralded by many supply chain role-players as the best hope to enable them to meet the increased need for in-transit visibility. Through the use of RFID, valuable information such as the shipment contents, its routing, and condition during transit (such as humidity and temperature) can be stored and transmitted to the relevant role-players. RFID technology has the potential to also serve as a basis for the development of improved container sealing technologies to ensure no tampering or unauthorised opening. The Smart and Secure Tradelane (SST) initiative mentioned above is an example of the use of such a technology. *"All these applications of RFID can potentially help to improve supply chain security and restore supply chain confidence, so that one can potentially achieve 'supply chain security without tears'."* (Lee, 2004)

Implication 4: Maintain agility and enhance ability to change

One of the major observations made and vulnerabilities of supply chains detected during 9-11 was the lack of agility and resilience of supply chains. Companies can

build in flexibility throughout their supply chains based on proven design principles and the right culture, in this way balancing security, redundancy and short-term profits. The focus should be on lowering vulnerability and increasing resilience.

Implication 5: Attention to both inbound and outbound supply chain activities and processes

Security throughout the entire supply chain is required including the various inbound and outbound processes. This requires visibility of the supply chain and interaction with supply chain partners and therefore links with implications one and three.

CONCLUSION

Given stringent security measures, increased investment requirements and heightened scrutiny of global trade, the news is not all doom and gloom. Now more than ever, countries are realising that they cannot go it alone: maritime security is everyone's problem, opportunity and responsibility alike. Closer collaboration, the free exchange of ideas, experience, knowledge and best practice are the best defence to achieve better security of supply chains. There is an undeniable link between the schools of thought on supply chain management and security and risk management. Both argue for the development, and management of, closer ties with trade partners and competitors alike. Both demand constant evolution, attention to detail, increased visibility, increased vigilance, sharing and commitment across international borders.

Where the developing nations of the world are struggling to achieve compliance, it is in the interests of international trade that developed nations offer expertise and assistance. Furthermore, reciprocal port visits, international forums and research must be encouraged to facilitate the sharing and adoption of best practices.

The trend worldwide seems to be towards holistic management of transportation risk, where the focus is shifting to encompass all modes of transport under the same umbrella and involve all role-players in supply chains in fostering the awareness that security is as vital a function of a supply chain as procurement, for example. For security to be truly efficient, it must be present at every step in the supply chain.

REFERENCES

Bichou, K., Bell, M.G.H. & Evans, A. 2007. *Risk management in port operations, logistics and supply chain security*. London: Informa.

Diop, A., Hartman, D., & Rexrode, D. 2007. *Customs-trade partnership against terrorism cost/benefit survey,*. Charlottesvillle: University of Virginia. Available online at: http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_cost_survey.ctt/ctpat_cost_survey.pdf 04/08/08

Emigh, J. 2005. Supply chain security poses opportunities, obstacles**.** E-week.com. September 23. Available online at: http://www.eweek.com/c/a/Supply-Chain-Management-and-Logistics/Supply-Chain-Security-Poses-Opportunities-Obstacles/ 04/08/08

Flynn, S.E. 2006. Port security is still a house of cards. New York: Council of Foreign Relations. Available online at: http://www.cfr.org/publication/9629, 04/08/08.

Lee, H.L. 2004. Supply chain security − Are you ready? *Stanford Global Supply Chain Management Forum*, SGSCMF-W1-2004 Available online at: http://www.stanford.edu/group/scforum/Welcome/White%20Papers/SC_Security.pdf, 04/08/08

Lyndon B. Johnson School of Public Affairs. 2006. *Port and supply-chain security initiatives in the United States and abroad.* Policy Research Project Report No 150., Austin: University of Texas..

National Board of Trade. 2008. Supply chain security initiatives: a trade facilitation perspective. Stockholm. Available online at: http://www.kommers.se/templates/Standard____3127.aspx 04/08/08

Sheffi, Y. 2001. Supply chain management under the threat of international terrorism**.** *The International Journal of Logistics Management*. 12(2): 1-11.

Available online at: http://esd.mit.edu/Headline/Terrorism-%20Sheffi-IJLM.pdf, 04/08/08

SITPRO. 2008. A UK review of security initiatives in international trade. London. Available online at http://www.sitpro.org.uk/policy/security/initiatives0108.pdf 04/08/08

Van der Merwe, C. 2006. Securing SA's ports. *National Ports Authority CEO Magazine*, 5(3).

wwwa. IMO. World Maritime Day 2005 International shipping – carrier of world trade,. http://www.imo.org/includes/blastDataOnly.asp/data_id%3D13168/backgroundpaper%28E%29.pdf, 04/08/08

wwwb. http://www.icc-ccs.org/prc/overview.php, 04/08/08

wwwc. http://www.homelandsecurityeu.com/pastissue/printarticle.asp?art=269629, 04/08/08

wwwd. www.imo.org, 04/08/08

wwwe. http://www.cbp.gov/xp/cgov/border_security/, 04/08/08

wwwf. US Customs and Border Protection. 2006. *Container Security Initiative, 2006 – 2011 Strategic Plan*, http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/csi/csi_strategic_plan.ctt/csi_strategic_plan.pdf, 04/08/08

wwwg. http://www.secureports.org/speeches/chris_koch_051705.html, 04/08/08

wwwh. http://www.logisticsmgmt.com/article/CA6492173.html?industryid=48468, 04/08/08

wwwi. http://www.dot.gov/affairs/dot10302.htm, 04/08/08

wwwj. Winston and Strawn. 2006. Congress enacts safe port act — port security legislation**,**. http://www.winston.com/siteFiles/publications/10-10-2006CongressEnactsSAFEPortAct.pdf, 04/08/08

wwwk. http://web.mit.edu/scresponse/, 03/07/08.

wwwl. http://www.stanford.edu/group/scforum/, 03/07/08.

wwwm. http://www.businessofgovernment.org/pdfs/GMM.pdf, 03/07/08.

wwwn. http://www.apl.com/news/documents/security_white_paper.pdf, 03/07/08.