



**HLSIA**

**Homeland Security Brief**

---

## Safeguarding International Trade



Donald C. Masters, Ph.D.  
Spring 2005

## Safeguarding International Trade

By Donald C. Masters, PhD

Advances over the last fifty years in trade liberalization, transportation technology and inland freight deregulation have made it possible to integrate markets on a global scale. The emergence of the “supply chain” and management innovations such as “just in time” inventories have lowered dramatically the costs of shipping and distributing merchandise. International trade, which normally grows at a faster pace than global GDP, underscores the growing interdependence of the world economy. International trade creates opportunities for greater specialization, economies-of-scale in production and distribution as well dynamic gains affecting markets worldwide. The end result is lower costs; a greater variety of products available and the productivity enhancing spread of newer technologies. Normally, countries with open trade regimes grow faster and enjoy higher incomes than those countries which discourage trade by imposing barriers of various kinds. The security challenge is to preserve the gains from trade while reducing the vulnerabilities implicit in the economic integration process.

What are the dimensions of safeguarding international trade from possible terrorist attacks? The very complexity of the intermodal transport infrastructure and global commercial relationships requires a risk management approach in order to avoid costly delays in cargo shipments. Thus, an effective security system must facilitate legitimate trade yet effectively target suspect shipments for inspection. The main area of concern is containerized shipping which is integral to international supply chains. Approximately, ninety percent of merchandise trade is shipped in containers<sup>1</sup>. There are an estimated 15 million containers in use around the world with roughly 7-9 million passing through U.S. ports annually<sup>2</sup>. The challenge of screening an average of some 20,000 containers a day for Weapons of Mass Destruction (WMD) or other potentially lethal threats is indeed a daunting task.

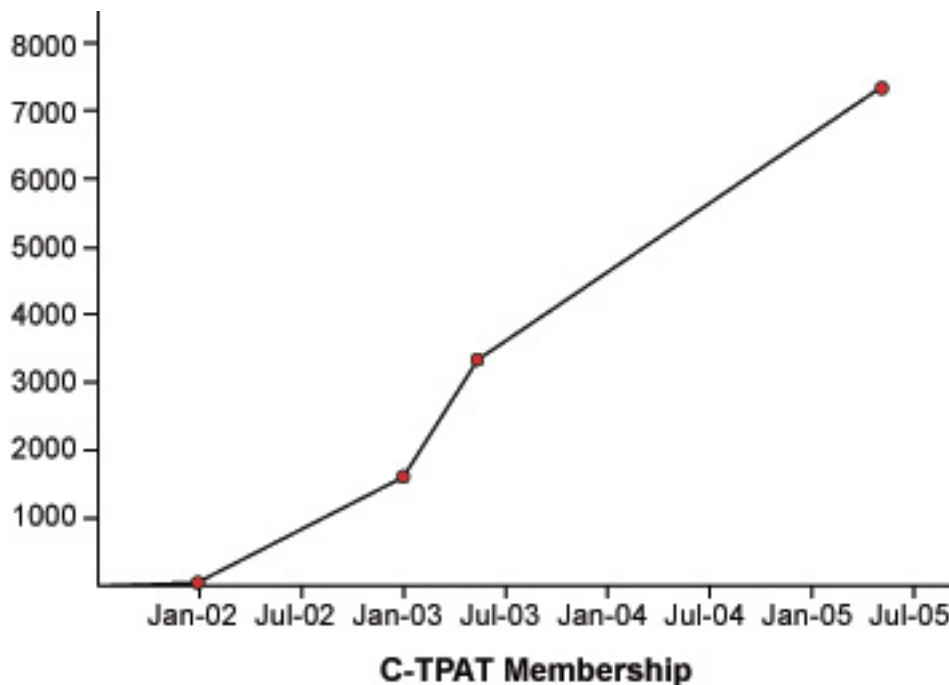
**U.S. Security Initiatives** – During the past four years since the 9/11 terrorist attacks, the United States has taken the lead in tightening port security through three important initiatives.

---

<sup>1</sup> “Container Security: Major Initiatives and Related International Developments”. United Nations Conference on Trade and Development. Commission on Enterprise, Business Facilitation and Development Seventh session. Geneva (24–28 February 2003). Pg. 6.

<sup>2</sup> “Securing the Global Supply Chain: C-TPAT Strategic plan”. U.S. Customs and Border Protection. <[http://www.customs.gov/linkhandler/cgov/import/commercial\\_enforcement/ctpat/ctpat\\_strategicplan.ctt/ctpat\\_strategicplan.pdf](http://www.customs.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf)>. pg. 12

1.) *Customs Trade Partnership Against Terrorism* (C-TPAT) is a joint government-business initiative aimed at building “cooperative relationships that strengthen overall supply chain and border security”<sup>3</sup>. Essentially, it is a non-contractual voluntary agreement whereby applicants complete the C-TPAT Supply Chain Security Questionnaire and sign a C-TPAT Agreement to Voluntarily Participate. The program requires participants to provide a security profile of their operations and encourage their business partners and suppliers to incorporate security recommendations/guidelines along the entire supply chain. Participants in the program benefit by receiving preferred customs treatment i.e. accelerated customs clearance. (It is estimated that non-participants are six times more likely to undergo inspection compared to C-TPAT “partners”.) The preferential relationship is based on US Customs gaining familiarity with the importer or shipper, which in turn leads to a lower “risk score”. The system is subject to periodic verifications and either party may withdraw from the program by simple notification. By May 2005, some 9,000 companies had applied for membership, roughly 7,400 companies had been accepted, and of these, 597 have been audited (verified) by Customs and Border Protection to insure that they had indeed improved their security systems<sup>4</sup>. Of the 7,400 partners, 86 of the top 100 importers by containerized volume, represent 96% of all US-bound container traffic<sup>5</sup>. C-TPAT has also been lauded by its proponents for its ability to reduce cargo theft and pilferage incidents. According to a study by the OECD, worldwide cargo theft costs shippers between \$30-50 billion per year.<sup>6</sup> By increasing security awareness of the location of containers and ships, companies can better identify vulnerabilities in their supply chain and work with their suppliers and subcontractors to address them.



<sup>3</sup> “CSI Fact Sheet”. Department of Homeland Security. Media Services. May 2005. pg. 1

<sup>4</sup> Lipton, Eric. “Loopholes Seen in US Efforts to Secure Ports”. New York Times. 25 May, 2005.

<sup>5</sup> “Securing the Global Supply Chain: C-TPAT Strategic plan”. U.S. Customs and Border Protection. Pg. 1

<sup>6</sup> As cited in Lukas, Aaron article. Pg. 8

2.) *Container Security Initiative* (CSI) works with foreign port authorities to inspect US bound shipping containers, of which 90 percent originate in thirty countries<sup>7</sup>. The goal is to improve security by pushing out the US security zone; thereby preventing terrorists and weapons of mass disruption from ever reaching the United States.

The CSI is a four-part program which includes:

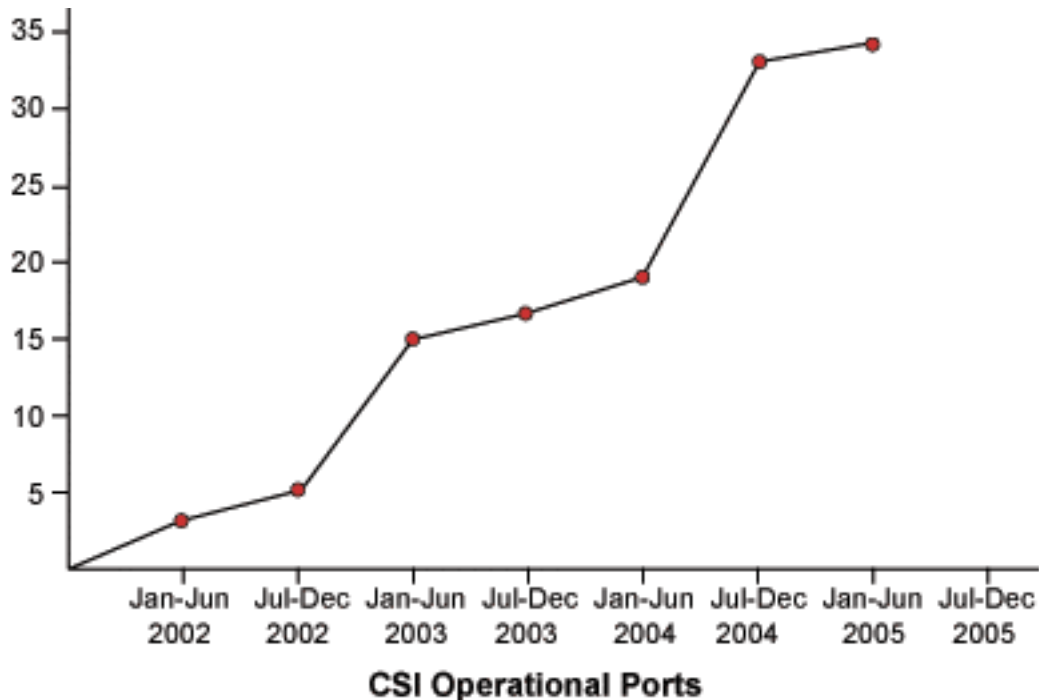
- establishing security criteria to identify high risk containers;
- pre-screening high risk containers before U.S. arrival;
- using advanced technology to pre-screen containers quickly and
- develop secure and “smart” containers.

Implementation of CSI requires bilateral agreements with the world's major ports. US Customs and Border Protection personnel, known as CSI teams, are assigned to foreign ports to supervise cargo containers being loaded on to ships destined for US ports. To avoid slowing down legitimate trade, the program uses intelligence sources and ship manifest information - Automated Targeting System (ATS) to *refer* suspect containers and their cargoes to host country customs officials for inspection. The referred containers may be inspected by non-intrusive means, such as x-ray or gamma-ray equipment. If warranted, the containers may be physically inspected. In the event that a “high risk” container that is referred to local customs is not inspected for whatever reason and inadvertently shipped, that container is placed on domestic hold for inspection upon arrival at the US port. The program, based on reciprocity, does not cover the costs of inspection equipment in the foreign port. Efforts are currently underway to improve detection devices such as the Radiation Portal Monitor (RPM) now being deployed in major US ports. A new objective is to establish minimum international standards for non intrusive scanning and imaging equipment. As of February 2005, 34 mega-ports worldwide are participating in the program<sup>8</sup>. Additional ports are applying to join the CSI program which includes meeting certain operational criteria, such as the deployment of an automated risk management system. Countries with certified ports include Canada, the Netherlands, Germany, Belgium, France, Sweden, Italy, Britain, Greece, Spain, Singapore, Japan, South Korea, Malaysia, Thailand, United Arab Emirates, China, South Africa and Argentina.

---

<sup>7</sup> “Container Security: Major Initiatives and Related International Developments”. United Nations Conference on Trade and Development. Pg. 6

<sup>8</sup> “Homeland Security: Key Cargo Security Programs can be Improved”. General Accounting Office. May 2005. <http://www.gao.gov/new.items/d05466t.pdf>. Pg. 9.



(CSI Fact Sheet; DHS. 2005)

3.) “The 24 Hour Advance Vessel Manifest Rule” is perhaps the most burdensome and controversial initiative launched to date by the U.S. Government. It aims at information collection and is closely associated with the CSI program. The goal of the “24 hour rule” is to identify prior to loading, those containers that are thought to be high risk. The rule was strengthened considerably under the U.S. Trade Act (2002) which imposes sanctions and penalties on shippers who fail to comply. As amended, the act requires the shipping community to provide advanced electronic information for cargo. Prior to 2002, only carriers participating in the vessel Automated Manifest System (AMS) were required to provide information electronically<sup>9</sup>. However, more recent regulations effectively oblige all vessel carriers operating in US trade to use AMS. Moreover, the requirement now includes both US exporters and importers. While technically only Cargo Declaration (CF-1302) needs to be filed 24 hours prior to container loading at the foreign port, considerable additional manifest information must be completed prior to arrival at the US port<sup>10</sup>. Finally, these regulations affect containers that are in transit to US ports<sup>11</sup>. In other words, containers transported on the same ship but are not off loaded at the US port are subject to manifest declarations and the 24 hour rule.

Recent U.S. Congressional hearings and GAO investigations have found deficiencies affecting key cargo security programs. In February 2005, the DHS inspector general criticized the method that his agency used to grant public funds to domestic ports, citing that smaller ports were disproportionately favored by

<sup>9</sup> “Container Security: Major Initiatives and Related International Developments”. UNCTAD. Pg. 12.

<sup>10</sup> “Current Maritime Developments”. Holland and Knight.

<http://www.hklaw.com/publications/maritimedevelopments.asp?Subject=portsecurity>. Pg. 5.

<sup>11</sup> Ibid.

grants, while critical ports such as Los Angeles and Long Beach had not received sufficient funds in order to effectively protect themselves in the event of a terrorist attack<sup>12</sup>. Moreover, Congressional hearings held in May 2005 questioned the operational effectiveness of some aspects of the CSI, C-TPAT programs. According to US customs officials roughly 10% of potentially risky containers had arrived at U.S. ports unscreened due to systemic problems<sup>13</sup>. It appears likely that these criticisms will result in a further tightening of DHS regulations.



**International Security Initiatives** - The international community has a large stake in protecting global trade valued at US\$7.5 trillion which is largely conveyed by ships carrying 6 billion tons of cargo each year<sup>14</sup>. It is estimated there are approximately 4,000 ports and a worldwide commercial fleet of some 46,000 ships engaged in international trade<sup>15</sup>. A terrorist attack on a vessel or a port can cause significant economic losses, both direct and indirect. The 2002 terrorist attack on the tanker *Limberg* did relatively minor damage to the vessel yet caused insurers to triple insurance premiums for vessels visiting Yemeni ports<sup>16</sup>. This resulted in diversion of ships to other ports ultimately causing Yemeni port terminals to close with estimated indirect losses equivalent to 1% of national GDP<sup>17</sup>. An incident at a mega-port could have ramifications both nationally and globally depending on the situation. A recent simulation (war game) of a terrorist incident resulting in the shut down of a major U.S. port generated direct and indirect costs estimated at US\$ 58 billion<sup>18</sup>. Securing the transport system which sustains international trade is a complex task particularly when a typical container shipment may involve 25 different actors, generate 30-

<sup>12</sup> Lipton, Eric. "Audit Faults U.S. for Its Spending on Port Defense". New York Times. 20 February, 2005.

<sup>13</sup> Lipton, Eric. "Loopholes Seen in U.S. Efforts to Secure Ports". New York Times. 25 May 2005.

<sup>14</sup> "Security in Maritime Transport: Risk Factors and Economic Impact." Organization of Economic Co-operation and Development. ". Maritime Transport Committee. Directorate for Science, Technology and Industry. July 2003. pg. 18.

<sup>15</sup> Security in Maritime Transport: Risk Factors and Economic Impact." OECD. pg. 7.

<sup>16</sup> Ibid. Pg. 7.

<sup>17</sup> Ibid.

<sup>18</sup> Gerencser, Mark, Jim Weinberg and Don Vincent. "Port Security War Game: Implications for U.S. Supply Chains. Booz, Allen and Hamilton. Washington D.C.: 2003. Pg. 6

40 documents and use 2-3 different transport modes spanning 12-15 different locations<sup>19</sup>. Clearly, international cooperation is essential to secure global supply chains in general and container shipping in particular.

The International Maritime Organization (IMO) has jurisdiction over containers at sea in international waters. The recently approved IMO package for security enhancements includes Safety of Life at Sea (SOLAS) Convention changes, specifically Chapter XI-2 dealing with ship security and a new 2-part International Ship and Port Facility Security Code (ISPS). The ISPS code details both mandatory as well as voluntary procedures, which became effective July 2004. The strategy is designed to improve the tracking of vessels, enhance ship and port security and ensure the integrity of containerized cargo. To implement the strategy there are five regulatory focus areas involving governments; ships; carrier companies, ports and certification/documentary requirements. Each focus area implies compliance costs associated with new regulations to enhance security. These costs relate to the additional personnel, equipment and training in new procedures required to meet the new security standards of the ISPS code. For example, governments are tasked with determining security levels (1-3) in national waters and communicating security level alerts to flag vessels both domestic and foreign. Depending on the risk level determination, certain mandatory procedures become effective for ports and ships in the affected areas. Operator costs are a direct function of the announced level of security. Moreover, ships must acquire additional equipment to enhance their security and train crew in security procedures. To ensure accountability and compliance ports, carriers and ship owners need to designate security officers responsible for meeting ISPS code standards. It is estimated that SOLAS/ISPS ship and company related costs are at least US\$1.3 billion initially and recurrent costs (mostly personnel related) at around US\$730 million annually thereafter<sup>20</sup>. In addition, there are assessments and plans that require ports to upgrade their security to better screen and secure cargoes as well as coping with direct threats. Due to the diverse conditions existing in the world's seaports it is difficult to estimate the cost of ISPS code requirements. However, the US Coast Guard estimated the cost for American compliance with SOLAS/ISPS at US\$ 5.97 billion in present value terms (US\$ 1.1 billion for vessel security and US\$4.87 billion for port security)<sup>21</sup>.

The United Nations Commission for Trade and Development (UNCTAD) has expressed concerns regarding the new security requirements, particularly as they relate to port costs and export market access<sup>22</sup>. Security costs may be high relative to less developed country resources. UNCTAD estimates that port ISPS compliance costs would be about US\$2.0 billion for less developed countries<sup>23</sup>. As a result, requirements related to pre-shipment container security and advanced electronic reporting of manifests may act as non-tariff barriers adversely affecting the trade prospects of developing countries. Already these countries are disadvantaged by higher-than-average world freight costs due to

---

<sup>19</sup> "Container Security: Major Initiatives and Related International Developments". Pg.24

<sup>20</sup> Ibid. pg. 35.

<sup>21</sup> Ibid. pg. 36

<sup>22</sup> Ibid.

<sup>23</sup> Ibid.

geographic location and inadequate transport infrastructure/services. In addition, transaction costs may be higher due to difficulties clearing customs or securing necessary permits and licenses. Thus, existing competitive disadvantages may be compounded by security-related measures recently imposed on third world exporters. Yet, by requiring that all IMO member countries comply with ISPS codes, underdeveloped ports may actually improve their efficiency and competitiveness in the long term.

In summary, new security measures impose significant compliance costs on the international shipping community. These costs relate to the fixed costs of new equipment and deployment of new technologies as well as additional personnel costs and administrative costs related to the extensive new manifest reporting requirements now mandatory for U.S. customs, i.e. AMS. These costs are not directly comparable to the economic costs associated with a major port shutdown which could be enormous. This is because a cost-benefit analysis to determine appropriate investment in security measures is not possible since the probability of a terrorist occurrence is unknown. Thus, security systems and their costs are based on strategic considerations related to risk management and closing obvious security gaps. Though cost estimates are still preliminary, they are significant in absolute terms particularly for less developed countries and smaller ports in developed countries. This poses level-playing field issues which are not easily resolved. Nevertheless, it should be kept in mind that security costs are extremely small relative to the value of merchandise traded in the world economy. They are unlikely to slow the longer-term trend towards greater global integration of markets.

---

### **Annotated Bibliography:**

#### **1. "Boxed in and Clogged Up". 14 October, 2004. The Economist.**

This article investigates the state of the major ports in the western countries, with special attention paid to Los Angeles and Long Beach due to their combined role as the U.S. ports with the most container traffic. Many major ports are experiencing congestion and lengthy delays due to the surge in imports from Asia. Much of this congestion is due to neglected and antiquated infrastructure; however Singapore and Hong Kong have been able to handle the increase of container flows through their facilities due to their heavy investment in new infrastructure.

#### **2. "Current Maritime Developments". Holland and Knight. <http://www.hklaw.com/publications/maritime/dev.asp?Subject=portsecurity>.**

The law firm Holland and Knight maintain an updated journal on legislative developments and events affecting maritime law, with a special section on cargo and port security regulations. There are useful summaries on court decisions, legislative activity, compliance, and port security. The information is updated regularly and the analysis of regulations is insightful. A good resource for background information and for keeping up on recent developments.

**3. Customs and Border Protection Office of International Affairs. "Container Security Initiative Fact Sheet". (2002 and 2005): 1-5. <[http://www.customs.gov/linkhandler/cgov/border\\_security/international\\_activities/csi/csi\\_fact\\_sheet.ctt/csi\\_fact\\_sheet.doc](http://www.customs.gov/linkhandler/cgov/border_security/international_activities/csi/csi_fact_sheet.ctt/csi_fact_sheet.doc)>**

The Customs and Border Protection Fact sheet on the Container Security Initiative (CSI) presents the official information [on this program], and attempts to answer some questions while addressing concerns over its impacts. The fact sheet goes over the history of the CSI, the progress that has been made to date, and the criteria for a port to become CSI listed.

**4. "Delivering the Goods". 13 November 1997. The Economist.**

This article analyzes the explosion in international trade, and explains its roots in the lowering of freight costs that has occurred in the latter half of the last century. Deregulation, containerization and intermodal transportation advances have led to productivity improvements. While deregulation in the U.S. began nearly 20 years ago, other parts of the world have highly regulated regimes. The article advocates that deregulation of the international shipping industry is also needed in order to truly bring the cost of freight down on a global scale.

**5. Dulbecco, Philippe and Laporte, Bertrand. "How Can the Security of the International Supply Chain be Financed? A Global Public Good Approach". Centre d'Etudes et de Recherches Sur le Developpement International (CERDI). France. Clermont Ferrand. (2003): 3-38.**

CERDI presented this report at the request of the World Customs Organization (WCO) in order to review the potential sources for financing the development of an international maritime security regime. The report is based on the theory that the security of the international supply chain is a global public good, and that it has direct consequences for the efforts of the WCO to promote trade facilitation in customs procedures. The authors argue that the efforts to strengthen the security of the global supply chain and to facilitate the international flow of goods are compatible, and that an expenditure on the former will result in a benefit to the latter. The report concludes that the World Customs Organization should coordinate an integrated network for financing and overseeing the establishment of a global regime on security and trade facilitation.

**6. Gerencser, Mark, Jim Weinberg and Don Vincent. "Port Security War Game: Implications for U.S. Supply Chains. Booz, Allen and Hamilton. Washington D.C.: 2003**

In October of 2002, the Washington branch of the consulting firm Booz, Allen, and Hamilton, hosted a Port Security War Game, which was attended by high ranking representatives from several Governmental agencies, CEOs of large firms, and experts in shipping and logistics. Basing their evaluation on a hypothetical terrorist attack on the port of Los Angeles/Long Beach, and a number of smaller U.S. ports, the participants estimated that such an event would cause as much as \$58 billion dollars worth of damage, and a backlog of containers that would take two months to clear.

**7. Lee, Hau L. "Supply Chain Security-Are you Ready". Stanford Global Supply Chain Management Forum (September 2002).**

Professor Lee has published a number of studies on the efficiency effects of incorporating security measures into supply chain management strategies. This article focuses on the benefits of reducing inventories, increasing visibility of the supply chain, and reducing lead times in customs and transit, and whether or not this can be accomplished by incorporating technology such as Radio Frequency Identification (RFID) tags on cargo and containers. According to the report, 75% of shippers anticipate having RFID deployed throughout their supply chain by 2006 or 2007.

**8. Lenain, Patrick, Marcos Bonturi and Vincent Koen. "The economic consequences of terrorism" Economics Department Working Papers. Organization of Economic Co-Operation and Development (OECD). No. 334. (2002): 23-32.**

Lenain, Bonturi and Koen study the myriad of economic impacts that the terrorist attacks of September 11, 2001 have had on the world economy. The scope of the report is very wide, covering short- and medium-term impacts of the attacks, including the increased costs to the insurance, airline, and shipping industries. The authors present the medium-term regulatory, trade and fiscal policy implications of the 9/11 attacks, along with a detailed analysis of the reaction by the insurance industry. The authors argue that security measures designed to prevent attacks on maritime cargo shipping will likely have stronger impact on developing economies as their exports tend to have higher transportation costs relative to the value of merchandise shipped and therefore, these measures will increase shipping costs more than in other countries.

**9. Lipton, Eric. "Audit Faults U.S. for Its Spending on Port Defense". New York Times. 20 February, 2005.**

Since its inception, DHS has given \$517 million in grants to improve the security at U.S. ports, but this money has not necessarily been given to the most vulnerable ports, according to the department's inspector general. A recent audit conducted by the department found that money has not been wisely spent in many cases, with grants being spread around as widely as possible, instead of focusing on the top 10 ports in terms of incoming containers. Port grants are only a small part of the \$2.5 billion that DHS has given to state and local authorities.

**10. Lipton, Eric. "Loopholes Seen in U.S. Efforts to Secure Ports". New York Times. 25 May 2005.**

Congressional officials have recently begun reviewing DHS regulations, such as C-TPAT, the 24-hour rule and the CSI, and criticizing what are perceived weaknesses in the programs. Notably, C-TPAT and CSI status have been granted to many private sector actors and ports without verifying whether or not they have tightened security as promised. Critics describe this program as "trust but don't verify". Out of the 5,000 applications that have been approved for C-TPAT membership, DHS officials have only verified that 597 companies have indeed improved their security infrastructure. Customs officials have agreed that there are areas where the systems can be improved, but say that the programs are a vast improvement over the pre-9/11 situation.

**11. Lukas, Aaron. "Protection without Protectionism: Reconciling Trade and Homeland Security". Trade Policy Analysis. Cato Institute.**

This white paper produced by the Cato Institute contains valuable information about the lead-up to the creation of U.S. supply chain security regulations as well as insight on the challenges of increasing security while maintaining efficiency. The author argues for private sector companies and consumers to meet the costs for securing the international supply chain, and for companies and logistics providers to incorporate technology improvements in their security strategies. Moreover, the author warns of the danger that these security measures may be used by domestic interests to press for unfair protection from foreign competition.

**12. “Opinion of the European Economic and Social Committee on the ‘Security of Transports’”. Official Journal of the European Union. 394th Plenary Session. C61/174. (24 October 2002): 174-183.**

The report assesses the impact of new security measures on the airline, insurance and maritime industries and offers a set of policy approaches that the European Union could take on these various issues. By the date of its publication, nine of the largest European Ports (which account for 22.5% of container traffic entering the U.S.) had agreed to comply with CSI requirements without consulting the European Economic and Social Committee (EESC). The report concluded that this would create unfair competition between ports, and as such it would be preferable to enter into an EU-wide agreement with the U.S. in order to cover all ports in this plan, thus avoiding any undermining of EU “solidarity”. As a result of this report, the EU has indeed signed an agreement that will eventually make all major EU ports CSI partners.

**13. “Reducing Trading Costs in a New Era of Security”. The World Bank’s Global Economic Prospects 2004: Realizing the Development Promise of the Doha Agenda. Washington, D.C. (2004): 179-203.**

The report makes the point that security measures can raise the costs of trading internationally in the short- to medium-term, but that in the long run they will most likely help to facilitate trade and promote efficiency, which will help to encourage export-led growth. While noting the potential trade facilitation benefits to be had from instituting these measures, the report recommends the involvement of multilateral organizations in the planning stages. Benefits include reducing the delays of clearing containers through customs and eliminating certain corrupt practices that currently stifle speedy and efficient customs procedures.

**14. “Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan”. Department of Homeland Security.**

This document contains the strategic plan, vision and goals for the future of C-TPAT. It was created by the Department of Homeland Security to explain and inform the public about C-TPAT. It provides a thorough background of the creation of the program, the potential benefits to partners, and the strategy for expanding C-TPAT to include more foreign firms, support other Customs and Border Protection Initiatives, and improve the administration of C-TPAT. Lastly, there is a brief overview of the expected costs to the public of this plan, as well as a list of performance measures. Department of Homeland Security (DHS) websites are also good resources for firms to become informed as to the eligibility requirements and application instructions for C-TPAT

partnership. DHS issued updated requirements for C-TPAT partners as of March 25, 2005.

**15. "Security in Maritime Transport: Risk Factors and Economic Impact. Organization of Economic Co-operation and Development. ". Maritime Transport Committee. Directorate for Science, Technology and Industry. July 2003.**

This report explores the risks posed to the international merchant maritime transport system by terrorist organizations. As a part of this vulnerability analysis, the paper explores the possible economic repercussions of a terrorist attack involving maritime transport. The second part of the paper explores the cost implications of security measures enacted in response to this threat, including the U.S. and multilateral initiatives.

**16. Shelby, Toby. "Shipping Industry steams for safe haven: The cost of meeting new security standards is high and those affected have a July deadline to meet". The Financial Times. (April 15, 2004).**

The focus of the article is the July 2004 deadline for ports to be certified as compliant with the International Ship and Port Safety code (ISPS), and the real danger that many ports around the world will not meet this deadline. The author notes that, by the April printing date, not only were many ports in developing countries not making progress on the requirements, but that many ports in the U.S. and Europe were struggling to meet the deadline. Furthermore, Andrew Webster of the TT Club, a maritime liability insurer, notes that the improved cargo checking resulting from the purchase of scanning devices reduces export tax fraud. Customs revenues in some ports increased as a result, and the transport of dangerous materials was controlled.

**17. Trade Act of 2002 Final Rule: Frequently Asked Questions. Customs and Border Protection. 3 August 2003.**

This resource is very useful for importers and carriers to understand the new requirements related to the 24-hour rule and the Automated Manifest System. There are questions related to how these regulations affect carriers, NVOCCs, break and bulk cargo, and other areas. It explains the data that is required and the time frames for notifying customs of the cargo that is being shipped to the U.S.

**18. "United Nations Conference on Trade and Security (UNCTAD) Secretariat report on Container Security and Related International Developments". UNCTAD Secretariat. (2004): 3-46.**

This report [by the UNCTAD secretariat] studies the various port and supply chain security initiatives, with a special focus on their potential impacts on developing countries. The report cites that 90% of the containers entering the U.S. originate from only 30 countries, several of which are developing nations. The report also notes that it is not clear who bears the cost of upgrading a port to the Container Security Initiative standards, especially in terms of non-intrusive imaging (NII) container scanner related expenses. These expenses could be covered by public or private funding, or they could be recuperated by charging exporters, importers, or other parties. Reportedly, most ocean carriers have begun to charge between \$25 and \$35 per bill of lading to

offset the increased costs associated with the 24-Hour rule, and that this adds to the already disproportionately high transport costs in developing countries.

**19. "When Trade and Security Clash". 4 April, 2005. The Economist.**

This article provides a very thorough introduction to the issues of security measures affecting containerized shipping, analyzing both the history of the intermodal transportation system, as well as the reasons why government officials are concerned about its exploitation by terrorists. The article lists some of the policy and technology recommendations that have been put forward to improve both the security and efficiency of international trade.

**20. Wills, Henry H. and David S. Ortiz. "Evaluating the Security of the Global Containerized Supply Chain". Rand Corporation. Infrastructure, Safety and Environment.**

This report uses a layered capabilities framework to analyze current supply chain security initiatives. Capabilities of the global container supply chain include efficiency, shipment reliability, transparency, fault tolerance and resilience. The report concludes that supply chain security and efficiency are distinct but interconnected, and that efforts to improve supply chain security may or may not have positive spillover effects in terms of efficiency. Furthermore, the report notes that all supply chain security initiatives have sought to improve the transparency of the system, while the authors believe that more focus on fault tolerance and resilience is needed. The study recommends that these areas be strengthened by both public and private initiatives, so that in the event of a terrorist attack on a major port, the economic impact can be mitigated. Lastly, the authors call for more research and development directed toward the creation of new technologies for low-cost, high-volume container scanning and tracking.

*This annotated bibliography was prepared by Nick Allen who is an HLSIA academic member and recently completed his Masters Degree in International Trade Policy at the Monterey Institute of International Studies. He will be working as a consultant in the field of supply chain security regulations.*