

Document: TILFWG 25-050  
Draft: **FIRST**  
Source: ABAC Canada  
Date: 27 July 2005  
Meeting: Kuala Lumpur, Malaysia

**Technology for Security and Its Impact on Trans-Pacific Supply  
Chains**

**Draft Report**

for

**APEC Business Advisory Council**

by

**Asia Pacific Foundation of Canada**

July 2005

## Table of Contents

Acknowledgements.....	3
Acronyms.....	4
Executive Summary .....	5
1. Introduction: The New Security Environment and Trans-Pacific Supply Chains .....	7
2. Objectives.....	9
3. Use of Technology in the New Security Environment .....	10
3.1. Security-Driven Technology at Ports .....	10
3.2. Security-Driven Technology in the Supply Chain .....	10
3.3. Other Security Measures.....	12
4. Benefits and Costs of New Security Initiatives .....	12
4.1. Outline of Benefits and Costs .....	12
5. Interview Approach and Structure .....	15
6. Results.....	17
6.1. Views on CSI, C-TPAT, and 24-Hour Rule .....	17
7. Samples of Interview Responses .....	22
8. Conclusions and Interpretations .....	26
Annex A: Interview Questionnaire for Container Security Initiative.....	27
Annex B: Interview Questionnaire for Customs Trade Partnership Against Terrorism .....	30
Endnotes .....	37

### **Acknowledgements**

We would like to thank Professors Carl Voigt and Dennis Schorr of the Marshall School of Business at the University of Southern California for their tremendous support on this project. Without their endeavours, we would not have been able to implement the in-field surveys and guide students at the Marshall School through the interview process.

We would also like to thank the 14 students at the University of Southern California for their efforts in tracking down interviewees and implementing the interview questionnaire. These students were: Chad Neault, Jorge Matheu, Sonny Wong, Eric Scholten, Julianne Wang, Xi Tan, James Carson Bo, Kaori Tsukamoto, Namrita Singh, Sunil Pradhan, Audrey Baca, Namrata Sharma, and Wooyung Joo.

We would also like to thank ABAC Staffers in the six APEC economies visited by these students-- Japan, China, Singapore, the United States, Korea, and Mexico-- for helping students make the connections with potential interviewees.

## Acronyms

APEC	Asia Pacific Economic Cooperation
BIC	Bureau International des Containers
CSI	Container Security Initiative
CBP	Customs and Border Protection Agency
C-TPAT	Customs-Trade Partnership Against Terrorism
fob	Free on Board
HKCTOA	Hong Kong Container Terminal Operators Association
IMO	International Maritime Organisation's
ISPS	International Ship and Port Facility Security Code
PECC	Pacific Economic Cooperation Council
RFID	Radio Frequency Identification
STAR-BEST	Secure Trade in the APEC Region Bangkok Laem Chabang Efficient and Secure Trade Project
TEU	Twenty Foot Equivalent Unit
US	United States
WMD	Weapons of Mass Destruction

## Executive Summary

As a response to the events of September 11<sup>th</sup> 2001, governments around the world have instituted significant security measures to help increase the security of containerized cargo while at the same time ensuring that legitimate trade continues. The United States' government's Container Security Initiative (CSI), its Customs Trade Partnership Against Terrorism (C-TPAT), and the International Maritime Organisation's International Ship and Port Facility Security (ISPS) Code are three such initiatives that have been implemented by various players in the supply chain in APEC economies.

While a number of studies on the economic costs of terrorism exist, global estimates on the costs and benefits of these new security measures are few and far between. Those that do exist rely on expert opinion to impute global costs or are based on specific programs such as APEC's STAR-BEST initiative. This study takes a different approach by interviewing important players in the supply chain in APEC economies to ask these players the costs they have incurred as a result of complying with new security measures.

For this study, we have interviewed representatives of 10 firms (so far) that represent some of the biggest ports, sea carriers, and exporting manufacturers in the world. Our broad conclusion is that, as far as established players in the supply chain are concerned, the new security measures have not had a major impact on their operations or profitability. This is because the large ports, carriers, and manufacturers already had the infrastructure and best practice systems in place to easily meet the new C-TPAT, CSI, and ISPS requirements.

We estimate that globally, total on-going costs of C-TPAT, CSI, and ISPS measures are around \$1.1 billion or \$4 per TEU. Over 80% of these costs are not specifically related to any of these programs but to the added costs associated with the so-called "24-Hour rule". In our view, therefore, C-TPAT, CSI, and ISPS have had a "light footprint" on the global supply chain.

In our view, the above estimates are at the low-end of the scale for two reasons. First, we have not interviewed firms in developing APEC economies and Small and Medium Sized Enterprises (SMEs). Including these firms in the sample would raise the average cost estimates significantly. Second, our cost estimates have not considered inventory costs at the receiving end of the supply chain (i.e., in the United States) which have elsewhere been estimated to be an order of magnitude higher.

Our interviews also provided insights into views of firms/ports on C-TPAT, CSI, and ISPS. As mentioned above, most of the firms we interviewed already had the best practices in place to become compliant with the new security environment very quickly. At the same time, both of the exporting manufacturers that were not C-TPAT certified considered becoming C-TPAT certified in the past, but did not see the benefits of achieving certification. This lack of benefit visibility was a common

theme among carriers as well. Carriers thought that C-TPAT was a base requirement of trading with the United States and as such did not see benefits such as reduced wait times, or increased volume of trade or throughput etc.

CSI partner ports had similar views. One interviewee likened the new security measures as “finding a needle in a hay stack” despite the use of new technology at ports. Again the view was that the new security measures was how business needs to be done in the post 9/11 world rather than seeing the benefits of the new security measures on productivity or the bottom-line.

## 1. Introduction: The New Security Environment and Trans-Pacific Supply Chains

Ocean containers play a vital role in international trade. The Bureau International des Containers (BIC) and Containerisation Online estimate that in 2001-02, approximately 15 million containers were in circulation and that these containers were moved 232 million times through ports worldwide. Nowhere is containerized cargo more important than in trade within the Asia Pacific Economic Cooperation (APEC) region. In 2002, 31 of the top-50 container ports in the world were in APEC economies, handling 141.9 million Twenty Foot Equivalent Units (TEUs). Seven of the top-10 container ports in the world were in APEC economies in 2002.

September 11th, 2001 was a watershed event for containerized cargo and the manner in which it will move across the oceans. With more than 50,000 containers arriving in the United States (US) every day<sup>i</sup> and nearly 50 per cent of the total value of all imports into the US arriving by sea<sup>ii</sup>, the US believes that in-bound cargo containers pose a significant threat to its national security. The Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) were two key programs initiated by the US government to help increase the security of containerized cargo while at the same time ensuring that legitimate trade continues. The CSI and C-TPAT have been complemented by the International Maritime Organisation's (IMO) International Ship and Port Facility Security Code (ISPS) that entered into force in July 2004. Together, the CSI, C-TPAT, and ISPS are the three newest and most important security initiatives underway at ports, sea and air carriers, and other parts of the international supply chain.

These security measures have resulted in a certain amount of debate within the international trade community in APEC economies. The CSI, C-TPAT, and ISPS all require a certain degree of investment in new technologies and processes. Exporters, carriers, and governments that may have been adversely impacted by them point to the costs involved in acquiring new technologies such as x-ray and gamma-ray machines, access control devices, risk management and container tracking software, and Radio Frequency Identification (RFID) technology. They also point to the lack of realizable benefits such as reduced inventory, insurance and pilferage costs, or reduced transit times, that may result from subscribing to the new security measures.

On the other hand, supporters of the use of these types of technologies have suggested that its benefits include not only enhanced security but also smoother flow of legitimate trade through the supply chain. Application of new security-driven technologies and procedures has the potential of driving efficiency gains that could result in net benefits to various players in the supply chain. APEC's STAR-BEST initiative which tested end-to-end supply chain security using RFID technology is a case in point. STAR-BEST was found to result in net benefits of \$220 per container (with an 80% probability). Globally, net benefits<sup>iii</sup> from implementing STAR-BEST would be \$3,300 million due mainly to greater supply chain predictability and timeliness of cargo shipments, transparency and process

improvements which allow importers to reduce transit time variations and inventory safety stocks.

Another example of potential benefits is a pilot project sponsored by the Hong Kong Container Terminal Operators Association (HKCTOA). Under this project, at an average speed of 15 kilometers per hour, every container arriving in two of the busiest terminals in the world-- Hong Kong's International Terminal and Modern Terminals-- passes through a gamma ray machine, a radiation portal, and optical character recognition cameras that record the container number. These images and radiation profiles are then stored in a database allowing the virtual inspection of all containers entering the terminal. At an average cost of \$6.50 per container, globalising this initiative would mean 100% scanning of container cargo at a cost of about \$1.508 billion with negligible reductions in transit times from past levels.

In the end, from the perspective of the private sector, the balance of firm-level costs and benefits of these programs dictate their efficacy and usefulness. Simply put, if programs are viewed as costly or overly prescriptive, than business will find a way around them or will pass on the costs to consumers. One case study of a Thai exporter undertaken by Pacific Economic Cooperation Council (PECC) researchers found that STAR-BEST was in fact viewed as imposing additional and unnecessary costs on Thai exporters with no obvious benefits. According to a Thai exporter interviewed by PECC researchers, for example, e-seals that are an integral part of STAR-BEST may not protect against theft since thieves sometimes use powerful levers to lift container doors entirely and others cut through roofs (or walls) of containers. The Thai case study also found that many of the other benefits such as reduced inventory costs, transit times, insurance costs, and better tracking of goods through the supply chain were not realized<sup>iv</sup>.

However, unlike the private sector, public policy-makers must also deal with the high costs of *inaction*. The potential risk of terrorists launching an attack by using containerized cargo is highlighted by the "Container Boy" incident, recounted here from *The Guardian*:

"He was well dressed, carried a laptop computer and appeared no different than any other business traveler except for the fact he had chosen to come to Canada in a metal box. Italian police arrested Amir Farid Rizk under new anti-terrorism legislation last week after finding him stowed away in a steel box on a container ship, on the eve of a three-week Atlantic crossing to Canada. Canadian officials were also alarmed, worried he might be a terrorist with a devious plan to sneak into the country undetected. His box was furnished with a bed and a bucket and was stocked with food and water. Mr. Rizk also had a satellite phone, maps and security passes for airports in Canada, Thailand and Egypt. He was traveling with a Canadian passport, which officials thought might be a forgery [this passport was later found to be valid]. He had not thought about air quality, and began pounding on the walls of his box after arriving in the Italian port from Egypt because he was having trouble breathing."<sup>v</sup>



The “Container Boy” incident highlights how terrorists can exploit security gaps in the global supply chain that relies on containerized cargo to enter, or worse, smuggle Weapons of Mass Destruction (WMD) into countries like the US. While threats exist in each step of the supply chain, these are particularly acute at the point of origination until containers are stacked onto ships. From the premises of the exporter to the loading docks of ports, for example, all it would take for a terrorist network would be to bribe a truck driver to take a long lunch. At ports, a lock-cutter or welding tools will get a terrorist or smuggler inside a container bound for their target country.

This tension between what the private sector views as being appropriate levels of transaction costs and what the public might perceive as potential risks is brought into stark contrast by a recently commissioned paper by the US Department of Transportation. This report<sup>vi</sup> found that a medium-scale atomic weapon, if detonated within or near a major US urban center would result in 50,000 fatalities, 300,000 injuries, and direct economic costs of nearly \$300 billion. While such quantitative measures will vary according to the assumptions used, from the public policy perspective, clearly, the potential costs of inaction are large and warrant some degree of intervention that may very well increase transaction costs to firms or prices to the end consumer.

## **2. Objectives**

Partly to address the various elements of this debate, in its Report to Leaders last year, ABAC proposed that a study be undertaken in 2005 to measure the impact of the new security environment on trade transaction costs. This report -- which is based entirely on interviews with ports, exporters, and sea carriers-- aims to not only arrive at global estimates of costs (and benefits) as perceived by various players in the supply chain but also provide case studies of how these players have been affected by the new security environment.

The overall objective of the project is:

- a) To arrive at global cost estimates of CSI, C-TPAT, and ISPS based on interviews of exporters, carriers, ports, and other players in the supply chain;
- b) To investigate the views of various players in the supply chain on the new security measures and how exporters, carriers, and ports in APEC have adopted to meet the new security requirements; and
- c) To assess how exporters, carriers, and ports in APEC have used technology as part of their change models.

### **3. Use of Technology in the New Security Environment**

#### **3.1. Security-Driven Technology at Ports<sup>vii</sup>**

Perhaps the most significant program in place at ports around the world is the Container Security Initiative (CSI). The key feature of the CSI is the posting of US Customs officials at major ports with the objective of pre-screening cargo destined for the US. Due to sovereignty issues, US customs officials do not have the authority to inspect cargo, relying instead on their counterparts from the host economy to undertake physical checks. Besides this physical presence, before a port can become a CSI partner port, it must implement the following standards:

- Customs Administrations at CSI Ports must be able to inspect cargo originating, transiting, exiting, or being transshipped through a country. Non-intrusive inspectional equipment (including gamma or X-ray imaging capabilities) and radiation detection equipment must be available and utilized for conducting such inspections. This equipment is necessary in order to meet the objective of quickly screening containers without disrupting the flow of legitimate trade;
- CSI Ports must establish a risk management system to identify potentially high-risk containers, and automate that system. This system should include a mechanism for validating threat assessments and targeting decisions and identifying best practices;
- CSI Ports must also share critical data, intelligence, and risk management information with the US Customs and Border Protection (CBP) in order to do collaborative targeting, and developing an automated mechanism for these exchanges;
- CSI Ports (and those conforming to ISPS codes) conduct a thorough port assessment to ascertain vulnerable links in a port's infrastructure and commit to resolving those vulnerabilities; and
- CSI Ports commit to maintaining "integrity" programs to prevent lapses in employee integrity and to identify and combat breaches in integrity.

As can be seen from the above description, technology is an important if not crucial component of CSI. From developing risk management systems to sharing intelligence to inspecting cargo, all CSI ports have gone through a rigorous audit process to ensure that they comply with the program's requirements. As of July 2005, 37 ports in 19 countries were CSI operational seaports. 15 of the 37 CSI ports were in APEC economies.

#### **3.2. Security-Driven Technology in the Supply Chain**

C-TPAT goes a few steps further than CSI (and ISPS) by trying to secure the entire logistics chain. It requires cooperation by importers, carriers, brokers, warehouse operators, and exporting manufacturers. C-TPAT certified firms are required to

have a verifiable plan in place for various aspects of trade security that results in some investments in technology. The core elements of C-TPAT's security recommendations as they relate to use of new technologies for Exporting Manufacturers, Air and Sea Carriers are the same. To become C-TPAT-certified, firms must have adequate:

- **Physical Security:** All buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include: Adequate locking devices for external and internal doors, windows, gates, and fences; Segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged, or otherwise fenced-in area; adequate lighting provided inside and outside the facility to include parking areas; separate parking area for private vehicles separate from the shipping, loading dock, and cargo areas; having internal/external communications systems in place to contact internal security personnel or local law enforcement agencies.
- **Access Controls:** Unauthorized access to the shipping, loading dock and cargo areas should be prohibited. Controls should include the positive identification of all employees, visitors and vendors and procedures for challenging unauthorized/unidentified persons.
- **Procedural Security:** Measures for the handling of incoming and outgoing goods should include protection against the introduction, exchange, or loss of any legal or illegal material. Procedural security controls should include: Having a designated security officer to supervise the introduction/removal of cargo; properly marked, weighed, counted, and documented products; procedures for verifying seals on containers, trailers, and railcars; procedures for detecting and reporting shortages and overages; procedures for tracking the timely movement of incoming and outgoing goods; proper storage of empty and full containers to prevent unauthorized access; and procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.

For Air and Sea Carriers, C-TPAT also recommends Conveyance Security and Manifest Procedures that are not part of the security recommendations for exporting manufacturers.

C-TPAT recommendations on security are extensive and open up many possibilities on the use of new technologies in the supply chain. For example access controls that require the positive identification of all employees, visitors, and vendors are most efficiently performed by e-card access devices and closed circuit television. Marking, weighing, counting, and documenting products bound for international trade can be performed by new inventory tracking software that is integrated with a firm's accounting systems. Container tracking devices that use GPS or RFID technology are increasingly being used to monitor the "timely" movement of in-bound and out-bound containers. In implementing Access Controls, for example,

exporting manufacturers are required to have a positive identification, recording, and tracking system in place for all employees, visitors, and vendors. For Procedural Security, C-TPAT requires procedures for affixing, replacing, recording, tracking, and verifying seals on containers, trailers, and railcars-- all of which may have a technology component

Due to its reach deep into the supply chain, C-TPAT is likely to be an expensive proposition for the private sector and the most difficult to verify. As of April 2005, only 9,038 firms were C-TPAT members, out of which 4,877 (or 54%) were certified.

### **3.3. Other Security Measures**

A separate, but equally significant, initiative that is designed to work in conjunction with CSI and C-TPAT is the US Customs requirement for the electronic transmission of detailed manifest information 24 hours in advance of a container's loading (the '24-hour rule'). This is being implemented to further improve the identification and targeting of high-risk containers, and applies to carriers in any country intending to send cargo to the US. Those containers which fail pre-screening, or for which manifest information is too vague or submitted too late, are issued with a 'Do Not Load' directive, which stays in place until the container satisfactorily meets all the requirements. Shipping agencies which fail to provide the required information in time face monetary penalties or civil claims for damages arising from delays in shipments, and vessels ignoring a 'Do Not Load' directive will be denied permission to unload the container at any port in the US.

## **4. Benefits and Costs of New Security Initiatives**

### **4.1. Outline of Benefits and Costs**

So, what are the benefits and costs of these security measures? As we show in Table 1, the major benefits from both the CSI and C-TPAT initiatives that are highlighted by US customs are the reduced border wait times due to reductions in the number of inspections, reductions in selection rates for trade-related compliance examinations; and more efficient inspections as a result of using x-ray and gamma-ray technologies. The added security measures could also reduce pilferage, insurance costs, tracking costs of containers, safety stock costs, and may result in reduced bill of lading surcharges. In addition to these quantifiable benefits, there are other measures that are inherently hard to measure. US Customs has indicated that if a terrorist incident involving sea cargo containers does occur, the US would allow trade with CSI ports to continue, but may refuse vessels and cargo from other non-CSI ports as a security measure. Obviously measuring the impact of such a measure is conditioned by the nature and severity of the terrorist attack.

An important economic benefit of these security initiatives is the non-quantifiable benefit of enhanced security. In our view, measuring the economic benefits of enhanced security is difficult, at best, since it involves assumptions that are hard to

validate within existing modeling frameworks. Nonetheless, the fact that security measures such as CSI and C-TPAT better ensure the integrity of containerized cargo does help improve confidence in the global supply chain whose impacts would be difficult to measure.

In terms of costs of implementing CSI, C-TPAT, and ISPS; the major costs are the incremental infrastructure costs related to complying with these security initiatives such as locking devices, fences, adequate internal and external communication equipment, identification and access control equipment, software and hardware to track containers, facilities to securely store empty and full containers, procurement costs for x-ray and/or gamma-ray machines, etc. To this, one must add the compliance costs of both being part of CSI and C-TPAT (from the perspective of host ports and supply chain participants such as exporters and carriers) and the costs of additional US customs officers stationed in overseas ports, staff costs related to on-going verification and audits of C-TPAT compliance, etc. Inventories accumulated at exporters' warehouses, and due to the additional lead times related to the 24-hour rule also need to be considered.

**Table 1: Potential Benefits and Costs of the New Security Environment**

<b>Benefits</b>	<b>Costs</b>
Reduced Border Wait Times Reduced Pilferage Reduced Insurance Costs Reduced Container Tracking Costs Reduced Safety Stock Costs Reduced BoL Surcharges ENHANCED SECURITY	Infrastructure Costs Compliance Costs Service Costs Inventory Carrying Costs PERCEPTION OF ENHANCED SECURITY

Finally, we should point out that an important, unquantifiable "cost" of security measures is the perception of enhanced security. An example from the Canada-US trading relationship will crystallize this point. Each month Canada exports 7,000 – 8,000 containers of municipal waste that enter the US through the Port of Huron<sup>viii</sup>. The density and variability of municipal waste is such that x-rays of trash containers makes it difficult, if not impossible, to identify anomalies such as weapons or other contraband. In this case, the impact of relying too much on x-ray and other types of technologies is that it would give a false sense of security, that if exploited by terrorists would have tremendous costs attached to it. Here we have a situation where a container could very well be classified as a low-risk container but is in fact a high-risk container. The benefit of added security clearly needs to be risk-adjusted.

## 4.2. Existing Estimates of Benefits and Costs of the New Security Environment

To our knowledge, there are very few global estimates of costs (or benefits) of programs such as CSI, C-TPAT, or the ISPS code. The estimates that do exist vary widely and are based on either expert opinion or specific modeling assumptions that result in varied estimates depending on assumptions used and program implemented. As an example, one estimate by the OECD puts the *costs* of the new ISPS code on sea carriers alone to be *at least* \$1,279 million initially and \$730 million per year thereafter<sup>x</sup>. APEC's STAR-BEST initiative, on the other hand, found net benefits of \$220 per container (with an 80% probability). Globally, net *benefits* from implementing STAR-BEST would be \$3,300 million<sup>x</sup> due mainly to greater supply chain predictability and timeliness of shipments, transparency and process improvements which allow importers to reduce transit time variations and inventory safety stocks. Such wide swings in potential benefits and costs (i.e., from +3.3 billion to -\$730 million) are entirely due to modeling assumptions.

It is important to put these costs in perspective and to use the correct base in the process. APEC's STAR-BEST initiative, for example, found that the on-going costs of deploying RFID technology would be \$86/container (on a capacity basis) or \$1.3 billion worldwide (i.e., \$86 x 15 million containers). Because implementing the ISPS code is mutually exclusive from STAR-BEST, cost estimates of roughly \$3.5 billion (we lump one-time costs of ISPS with on-going costs for the sake of argument) for "securing" global trade in the trillions of dollars does not seem like a significant cost to the trading system. However, the shipping industry will typically use the total container capacity of about 15 million containers as the base to translate this into costs per container. If we use this capacity measure as the base, total estimated costs of these two initiatives works out to about \$220 per TEU (on a capacity basis). As a reference, the carrier cost of shipping a container eastbound from Shanghai to Vancouver is about \$2,400 (which includes port charges). Carriers, therefore, argue that at 10% the new security environment will pose a significant added transaction cost to international trade.

But these 15 million containers move about 230 million times in any given year. So, if we use this "volume" measure as the base, the total estimated costs of these two initiatives works out to about \$12 per TEU on a volume basis.

Another base that one can use is the value of the goods carried in these containers. Large retailers such as Wal-Mart, Target, Hudson Bay (Canadian retailer) typically carry products worth about \$60,000 in these containers. Even at an additional \$220 per container, overall costs are about 0.4% of value of shipments in an average container imported by Wal-Mart or Target.

While estimates on the economic impact of terrorism vary considerably (it is not within the scope of this paper to review this literature), recent research has zeroed in on potential direct and indirect costs of a terrorist attack on shipping, maritime infrastructure, or on countries themselves. The most significant incident that highlights impacts on a developing economy was the October 2002 attack on the

French oil tanker *Limberg* off the coast of Yemen. In the aftermath of this attack, underwriters tripled insurance premiums for vessels calling on Yemeni ports. At as much as \$250 per TEU, these premiums led some lines to cut Yemen from their schedules. Others shifted to ports in neighbouring countries. Yemeni ports saw throughput decline from 43,000 TEUs in September 2002 to 3,000 TEUs in November 2002 with as many as 3,000 people losing their jobs as a result. The Organisation for Economic Co-operation and Development estimates that the *Limberg* incident cost the Yemeni economy 1% of its 2001 GDP<sup>xi</sup>.

Another (and in our view, important) measure of costs to business is the movement by manufacturers away from “just-in-time” deliveries toward “just-in-case” inventory holdings. David Closs at Michigan State University estimates that in 2002, average large American companies held 1.43 months worth of inventory, up from 1.36 months of inventory in 2001<sup>xii</sup>. Closs estimates that the increased inventory holdings could add \$50 billion to \$80 billion to business costs in the US alone in 2002 or 0.5% - 0.8% of 2001 US GDP.

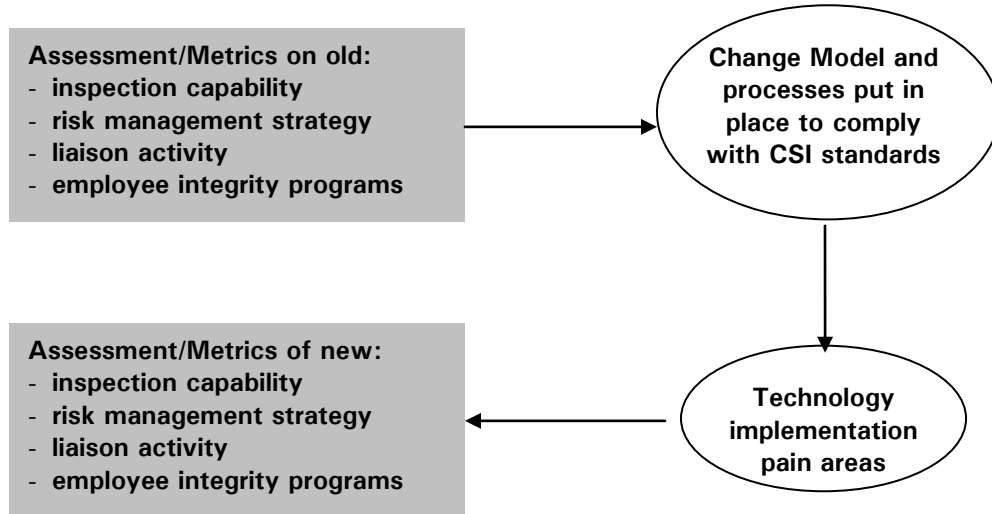
Aside from these overall measures, there has been no systematic effort at determining cost estimates based on surveys or interviews of the private sector itself. In that sense, we feel that the current report adds value to the literature, as it is based entirely on estimates arrived at through interviews of some of the leading ports, sea carriers and exporters in the APEC region. Further, as a result of these interviews, we have been able to shed some light into the change models deployed by exporters, carriers, and ports in APEC to meet the new security requirements and assess the extent to which exporters, carriers, and ports in APEC have used technology as part of their change models.

## **5. Interview Approach and Structure**

Because CSI and parts of ISPS are focused on ports, the target interviewees were high-level officials in port authorities at participating CSI ports. As mentioned above, 15 of 37 CSI partner ports were in APEC economies with 12 ports in Asia. Thus far, we have interviewed officials at 3 of these ports. These ports fall within the Top-10 container ports in the world.

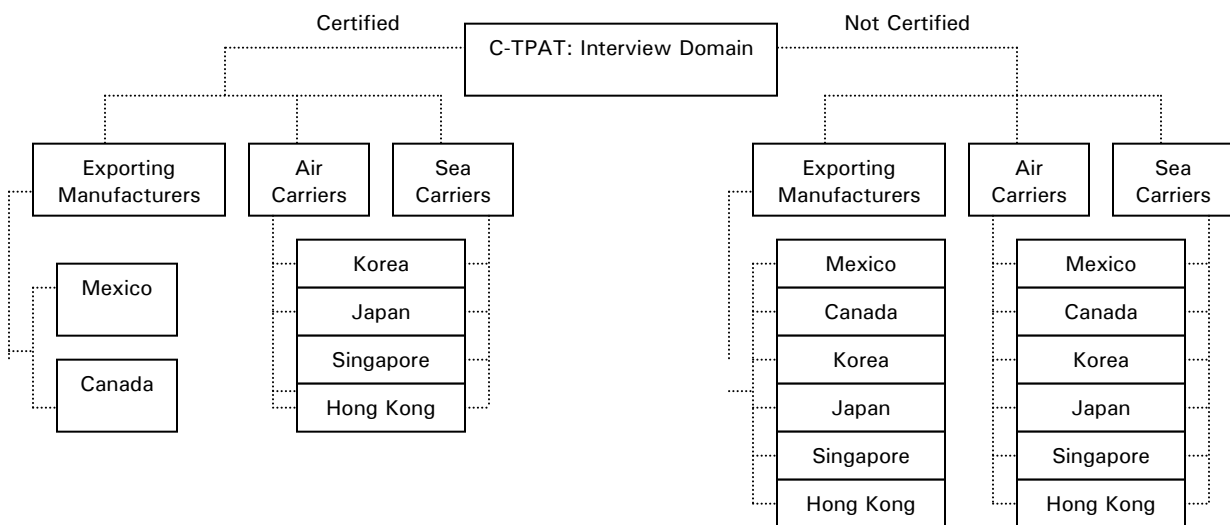
The overall interview approach with port authorities was to assess pre-CSI capabilities in areas such as inspection, risk management strategy, etc. and compare these with post-CSI standards. An important element of the interviews was also to assess the change models used by port and customs authorities to implement CSI standards described in section 3.1 above. This involved interviewing multiple players that are responsible for customs inspections, risk management, liaison with U.S. authorities, and employee integrity programs. The overall interview structure for CSI interviews is described in Figure 1 below. The interview questionnaire for CSI appears in Annex A.

**Figure 1: CSI Interview Structure**



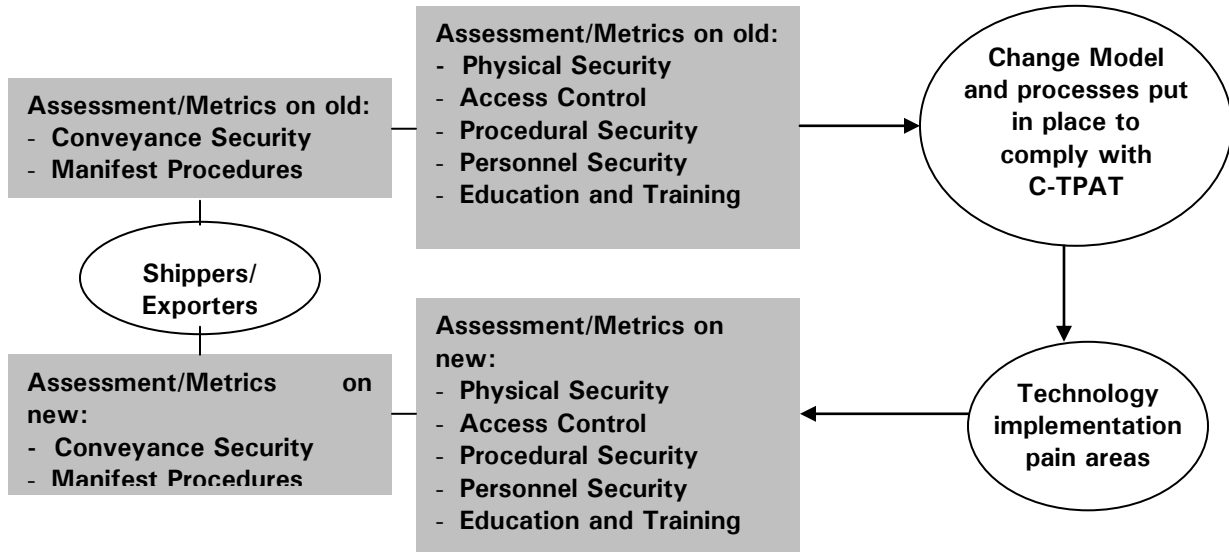
Because C-TPAT is a voluntary program and US CBP does not disclose the names of participating companies, we relied on firms to voluntarily disclose their participation in the program. We, therefore, divided the questionnaire into two categories-- one for firms that are C-TPAT certified and one for firms that are not C-TPAT certified (see Figure 2 below). C-TPAT also affects Licensed Brokers, Air Carriers, Sea Carriers, Rail Carriers, Air Freight Consolidators/Ocean Transportation Intermediaries, etc. For this project, we only interviewed exporting manufacturers and sea carriers since these would be most affected by Trans-pacific container trade (see Figure 2). So far, we have interviewed four manufacturing exporters (2 C-TPAT certified, 2 not certified) with an average revenue of \$133 billion and three sea carriers (all C-TPAT certified) with average revenues of \$9.6 billion. Together these firms represent some of the largest exporters and carriers of finished goods and containers in the world. The interview questionnaire for C-TPAT appears in Annex B.

**Figure 2: Interview Approach for C-TPAT**





**Figure 3: C-TPAT Interview Approach**



The methodology and questionnaire for interviews was developed in close cooperation with the University of Southern California’s Marshall School of Business. The questionnaire is currently being implemented by 14 University of Southern California students that are on assignment in various positions in the Asia-Pacific. In all, therefore, a total of 10 interviews have been conducted thus far. From this initial sampling, we are confident that the global estimates that we describe below are based on data from some of the most important players involved in trans-pacific supply networks.

## 6. Results

### 6.1. Views on CSI, C-TPAT, and 24-Hour Rule

Based on interviews conducted thus far, the overall conclusion that we can reach is that players in the supply chain (i.e., ports, customs authorities, carriers, and manufacturers) do not view C-TPAT or CSI as having an overly positive or negative impact on their operations. Most of the issues we heard during interviews related to the 24-hour rule. While most players did incur incremental costs related to C-TPAT and CSI, these were considered to be minor relative to the size of the firm.

For sea carriers there were no major incremental costs as a result of C-TPAT certification. For sea carriers we interviewed, most security requirements were

already in place prior to C-TPAT. All three Sea Carriers viewed C-TPAT as having no significant positive or negative impact on the volume of their US business.

We heard a similar view from ports and customs authorities regarding. The authorities interviewed did not view CSI as having a significant impact on their operations including on issues such as transit times. It is significant to note that one authority mentioned that they bought gamma-ray units at a cost of \$3.75 million and \$650,000 in supporting infrastructure. This works out to a one-time cost of \$0.22/TEU (on a volume basis) passing through that port. To our surprise, there were no additional staffing costs required as a result of CSI.

The manufacturers we interviewed did not have any problems meeting C-TPAT certification and did not incur any additional costs. If anything, the 24-hour rule increased lead times for these manufacturers by 2 days. This delay lead to additional lead-time costs of, on average, \$1.8 million per year. The manufacturers also provided costs associated with overflow at port yard of, on average about \$13 million per year, which was a negligible share of the average \$133 billion in sales recorded by them.

## 6.2. Imputed Global Costs

In going from the firm-level fixed and variable costs provided to us by our interviewees to overall global costs, we assume that the agents interviewed are representatives of their overall industries. Therefore the per TEU figures of their fixed and variable costs can be imputed and attributed to them to their portion of the supply chain globally. One weakness of this approach is that our sample does not include small and medium sized enterprises (SMEs) that, in our view, would incur greater costs per dollar exported. So, the estimates we are providing are in the lower end of the cost range.

At the same time, however, the diversity of estimates obtained gives us three separate levels of global costs-- low, average, and high. An example (see Table 2) will clarify the methodology we used to impute global costs. The three carriers that we interviewed mentioned that their fixed costs were between \$925,000 - \$1.4 million in upgrading their office infrastructure. From annual reports, we know the volumes handled by these carriers. By dividing overall infrastructure costs by volumes handled, we get the costs per TEU for that carrier. Now, we know the total global volume of container traffic. By multiplying the costs per unit with overall quantities, we obtain three scenarios of overall global costs—low, average, and high (we only report the average figures here).

**Table 2:** Imputing Global Costs-- Methodology

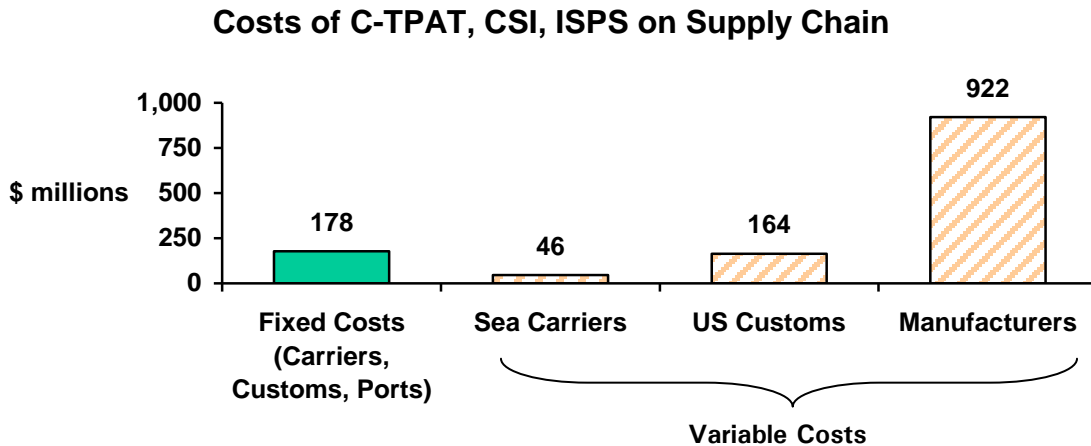
	<b>CARRIER A</b>	<b>CARRIER B</b>
Fixed Costs—Infrastructure	\$925,000	\$1,400,000
Volumes in 2004 (TEUs)	1,000,000	1,000,000
Fixed Cost (\$/TEU)	\$0.925	\$1.40
Global Volume in 2004 (TEUs)	232,000,00	232,000,00

Total Global Costs (\$ millions)	\$214.6	\$324.8
----------------------------------	---------	---------

Based on interviews thus far, we found fixed costs of complying with C-TPAT, CSI and ISPS to be fairly small at about \$175 million. 72% of these fixed costs are incurred by carriers in complying with C-TPAT requirements including in upgrading access controls to office spaces to include electronic e-card key access, additional points of observation for CCTVs, vessel upgrade costs for container vessels VSP and hardware upgrades. 28% of fixed costs-- approximately \$50 million-- were related to the purchase of x-ray and gamma-ray machines and related infrastructure.

We estimate that the total variable (or on-going) costs are about \$1,130 million. Over 80% of these costs (\$922 million annually) are incurred by exporting manufacturers. Significantly, most of these costs to manufacturers are associated not with CSI or C-TPAT but with the 24-hour rule. All four manufacturers we interviewed mentioned how the 24-hour rule has increased lead times for them and increased inventory carrying costs and port gate charges. We have also included costs of implementing CSI and C-TPAT by the US government, which have a budgetary allocation of \$164 million.

**Figure 4: Global Cost Estimates**



Source: APF Canada.

### Case Study #1: CSI Partner Port

**Security Measures Prior to CSI:** Before this port became a CSI partner port, it did not have scanning or x-ray equipment in place. According to the port official we interviewed, revenue collection was the primary objective of customs while security of cargo going through this port was a secondary objective. The port, however, did have an automated risk management system in place although the focus of the system was to identify shipments that violated reporting, import, and intellectual property laws. Again, security was not a focus of the risk management system. The port utilized a two-tier pre-clearance system that looked for red flags that would indicate that the container should be examined by customs officials in further detail. Examples of potential flags were high-risk countries, high-risk importers, first-time importers, incompatibility between importer and contents on the bill of lading, etc.

To inspect containers, the customs authorities would physically examine the contents of the container. The physical check, however, typically did not go beyond the opening of the container and examining the contents near the doors. Contents deep inside the containers were rarely examined. Prior to CSI, only 1% of inbound containers were inspected at this port.

There was also a limited sharing of information with the US prior to CSI implementation. There was no direct communication with US authorities. When information was deemed to be of interest to the US, it was passed through internal channels within the ports' customs channels. If senior customs officials concurred that the information was relevant and should be passed, they would pass it along through direct communication with the US Embassy.

**CSI Implementation Experiences:** To become CSI certified, the port invested in scanning technology and related infrastructure such as inspection platforms, scanning stations, sheltered platforms, and an office unit. Each of its scanning unit requires 3 officers for operations. All officers were trained on the equipment with no new officers hired. There were, therefore, no additional operating expenditures. It now takes approximately 1 minute to scan a 40 foot container with 200-300 containers scanned every day.

In terms of Liaison with the US, the port does not have any software or electronic links with US authorities. CSI officers are stationed at the port allowing for personal communication. CSI officers have some access to the port systems to assist in clearing US-bound cargo. The requests of US customs agents to further examine containers are passed along to local customs agents through a paper-based system. Only requests related to security or terrorism threats are considered by local authorities. The costs of the facility to host CSI agents was born by the port but no quantifiable value was provided by the interviewee. No rent is charged to the US for office space. Similarly, scanning, hoisting, trucking to and from the scanning station is done free of charge. A nominal fee is charged to the US for access to the ports' operating system. Costs of unstuffing a container is \$180 -\$240 which is passed on to the carrier. After CSI implementation, 10% - 15% of inbound containers are currently being inspected through the port's scanning equipment.

**Opinions on CSI:** The official we interviewed did not feel that the port experienced any increase in its trading volumes with the US as a result of CSI implementation. According to this official, the port's clients trade with the port because of its efficiency and productivity and not because of benefits CSI might provide in expediting shipments through the port. The port did not experience any delays in outbound or inbound cargo resulting from the use of its scanning technology. Shipment times from port-gate to ship-hull also remained the same. The official also did not identify any key pain areas related to CSI implementation. Scanning equipment, on the other hand, has helped identify containers carrying counterfeit goods. The official thought that by installing new technology, goods moving through the port were more secure. But he did mention that even with the new technology, "Security measures are still like finding a needle in a hay stack."

### Case Study #2: C-TPAT Certified Carrier

**Security Changes Made as a Result of C-TPAT:** This large carrier has upgraded its access controls to its office spaces to include electronic identification card access in many locations. All visitors must now pass reception control where their photo ID is examined. Visitors are now issued with visitor passes and are escorted within the firm's facilities. Visitor passes and logs are updated when the visitor enters and exits the firm's premises. Employees are also issued with photo ID with RF cards to access the firm's facilities. Closed Circuit Television, which was widely used prior to September 11<sup>th</sup>, is now being deployed more intelligently and additional points of observation are now included as a result of the C-TPAT program and preparation for the validation inspection. Lighting perimeters and clearing of fences have also been incremental expenses resulting from ISPS upgrades. Approximate costs of these upgrades was \$25,000 per office and \$200,000 at Head Quarters.

The firm has not made any changes to security measures in place prior to C-TPAT to protect against un-manifested material being introduced into vessels operated by the firm or providing advance information to US authorities on crew and passenger lists. The company has reinforced its Known Shipper Policy to its sales, documentation, and customer service staff which protects against any un-manifested material being introduced into its vessels. The firm participates in the Electronic Notification of Arrival (E-NOA) program of the US Coast Guard that provides passenger and crew lists to US authorities. The executive interviewed did mention that the ships that did not have e-mail capability were equipped with it to ensure that E-NOA requirements were met.

The executive interviewed did mention that the Carrier maintained state of the art Safety and Environmental Management Policies and Procedures under its ISO 9000 program. C-TPAT and ISPS required only minor changes to their existing program. There were no other significant changes as a result of the C-TPAT program.

**Opinions on CSI:** The executive we interviewed felt that C-TPAT did not result in increased trade volumes to the US. C-TPAT, in his opinion, was a base requirement to trade in the US and there were no significant benefit for carriers to comply with C-TPAT requirements. The executive mentioned that he expected an increase in quotation of charter rates in upcoming contract renewals as owners of vessels will begin assessing the incremental costs for past or anticipated security upgrades. The executive also made the point that because they were a large carrier with best practices already in place, that their costs may be "unusually low as compared to average sea carrier cost[s]".

## 7. Samples of Interview Responses

Below we provide a sampling of what we heard from interviewees. Please note that since most interviewees did not want themselves or their organizations identified, we have removed references that would allow any attribution to the individual comments.

### Carrier A

**4) C-TPAT has a number of recommendations on Physical Security, Access Controls, Procedural security, and Personnel Security, Conveyance Security, and Manifest Procedures for sea carriers. Did your firm make any changes to its existing security program to become C-TPAT certified?**

"Access control to office space has been upgraded to include electronic photo I.D. card key access in many locations. CCTV although widely used prior to 9/11 upgrades is more intelligently deployed and additional points of observation are now likely included as result of C-TPAT program and preparation for Validation inspection. Lighting and clearing of fence lines have been incremental expense exposure during ISPS upgrades.

Combined vessel upgrade cost for container vessels VSP and hardware upgrades yields an annual cost of less than 2 USD per TEU. It should be noted that we could expect higher quotation of charter rates in upcoming renewals as owners will likely attempt to assess incremental costs for past or anticipated security upgrades.

We have maintained state of the art Safety and Environmental Management Policies and Procedures under its ISO 9000 program known as NAV9000. C-TPAT and ISPS required only minor changes to our existing program. Our cost may be unusually low as compared to average sea carrier cost."

**10) In your opinion, has C-TPAT resulted in increased trade volumes by your firm to the United States?**

"No, C-TPAT is a base requirement to trade in the United States. There are no benefits for Carriers."

### Carrier B

**12) What are your overall opinion on C-TPAT and its impact on your firm's business?**

"It's a necessary part of doing business, since many customers require their sea carrier to be C-TPAT compliant. C-TPAT is a means to secure the supply chain in the containerized trade has a necessary place, but it appears that role is still up for debate within the US government, as well as other international organizations."

### Port Authority A

**15) What are the key pain areas in the use of technology that your port has experienced as a result of the CSI and ISPS initiatives?**

"Initially, there were concerns about high inspection cost and delays but no issues so far. There is only about 1 inspection per day."

**Port Authority B**

**10) How does your port now liaise with U.S. Customs? What type of technology does your port authority deploy to share information with U.S. Customs? Were there any additional costs involved? If so, How much?**

"There are no software or system linkages between the two countries. CSI officers are stationed at the port allowing personal communication. The US customs agents have some access to the port systems to assist in clearing United States bound cargo. The requests from US customs agents to further examine containers are passed along to the port customs agents through a paper-based system. Only requests related to security and terrorism threats are entertained.

The cost of the facility to host the US CSI agents was born by the port but no quantifiable value can be ascertained. No rent is charged to the US for office space. Similarly scanning, hoisting, trucking to and from the scanning station is done free of cost. With scanners as much as 10 -15% of inbound containers are currently being inspected.

A nominal fee is charged to the US for access to the ports' operating system. Cost of un-stuffing a container is approximately US \$180-240 which is passed on to the shipping line."

**13) In your opinion, has CSI and ISPS resulted in increased export volume from your port?**

"No, any increase is attributable to the global phenomenon of increased trade. Customers trade through the port because of productivity and efficiency not because of supposed benefits CSI might provide in expediting shipments through the port."

**16) In your opinion, have technological investments made by your port authority as a result of CSI and ISPS been beneficial to the movement of goods through your port?**

"Only in the sense that the goods are more secure. The quickest movement of goods through the port would be achieved in the absence of customs or scanning, but that is not realistic. "Security measures are still like finding a needle in a hay stack."

**Manufacturer A**

**11) What are the key pain areas in the use of technology that your firm has experienced as a result of the C-TPAT initiative?**

"Impact of 24 hour rule

Before: custom clearance and loading was 1 day. After: 3 days

- 1) Made up time between order receive and data entry
- 2) Worked overtime
- 3) Forwarder worked longer

- 4) Extra charge 5pm + , Saturday and Sunday
- 5) Inventory rose and impacted settlements
- 6) Space constraint in container yard."

**12) What are your overall opinion on C-TPAT and its impact on your firm's business?**

"The firm would willingly consider participating, but they see no benefit (streamlining, boosted revenue) to their business (other than complying with the wishes of U.S. counterparts)."

**Manufacturer B**

**12) What are your overall opinion on C-TPAT and its impact on your firm's business?**

"The company considered preparing for C-TPAT but could not see clearly the risk involved in not becoming C-TPAT certified. Tremendous time and costs involved in following the C-TPAT Foreign Manufacturer Security Recommendations would not be justified unless the risk of not following them becomes clear.

The company decided not to apply for C-TPAT in 2003 after consultation with lawyers because the risk of not becoming C-TPAT was not clear.

Even now, the risk is not so clear that the company does not have an idea of becoming C-TPAT certified.

Therefore, there are almost no changes or impacts on the company's security measures of C-TPAT."

**Concerning the 24-hour rule**

"The 24 hour rule affected the sea carriers, not the exporting manufacturer except that the shipping schedule for the exporting manufacturer became a bit tighter than before. The company doubts the effectiveness of the 24 hour rule. The rule has tightened the shipping schedule but are there any fruit of submitting data 24 hours before?"

The company does not take special security measures for both exporting and importing goods other than the usual security measures such as security checks at the entrance of the buildings though it considers it important to prepare for C-TPAT.

The company will consider preparing step by step for C-TPAT as necessary measures taken by exporters under C-TPAT become clearly defined."

**Manufacturer C**

**Concerning the 24-hour rule**

"In 2003, the U.S. started to request sea carriers to submit the details of containers based on each B/L to AMS in the U.S. 24 hours before leaving port. It takes 48 hours for sea carriers to prepare data so the shippers have to submit data 72 hours before, meaning that the lead time for shippers has increased by two days.



As for the air cargo, in 2004, the U.S. started to request air carriers to submit the details of cargos to the U.S. Customs 4 hours before the arrival.

As shown above, there is a lead time difference between sea cargos and air cargos. The company understands the U.S. security policy but wishes that the requirement for the sea cargos would be moderated to the same dead line for submission as by air cargos.”

## 8. Conclusions and Interpretations

This study is the first of its kind (that we know of) that arrives at global cost estimates of implementing CSI, C-TPAT, and the 24-hour rule based on interviews with various players in the supply chain. With on-going cost estimates in the \$1.1 billion range, we estimate that global costs are in the \$4 per TEU range (on a volume basis). While these are additional costs to various players in the supply chain, we think that they are small enough to be absorbed by consumers and/or manufacturers without a significant impact on consumption patterns or profitability.

Our conclusion on global cost estimates must be interpreted with caution for several reasons. Our sample of ten (so far) is not only small, it also consists of some of the largest ports, carriers, and exporters involved in cross-Pacific trade. Most of these players already had the infrastructure and systems in place to implement CSI and C-TPAT quickly and without significant additional investments. We therefore think that as smaller ports, carriers, and exporting manufacturers are included in the sample, that the \$4 per TEU cost estimate will increase. However, even with a tripling of this figure to \$12 per TEU, for example, these incremental costs amount to only 0.02% of the value of goods bound for retail outlets like Wal-Mart and Target in the United States or 0.5% of overall shipment charges for east-bound containers across the Pacific. More importantly, we have not taken into account important costs that were beyond the scope of this paper. These included the movement from “just-in-time” to “just-in-case” inventory holdings that some analysts have suggested would have an impact that is several orders of magnitude higher than our estimates.

Our interviews, however, reflected the “light footprint” of both the CSI and C-TPAT initiatives. In all our interviews, firms or customs authorities felt that they already had the capability to meet program requirements and any adjustments they made were minor. The biggest complaint we heard was related to the 24-hour rule from exporting manufacturers who felt that this rule would unduly increase costs to them.

However, we would also like to note that in all of our interviews firms did not realize the major benefits of CSI or C-TPAT such as reduced wait times, reduced pilferage costs, reduced insurance premiums, reduced bill of lading surcharges, etc. This, in our view, is significant because two manufacturing exporters chose not to become C-TPAT certified precisely because they did not see the realizable benefits of joining the program, despite having the capability to do so.

## Annex A: Interview Questionnaire for Container Security Initiative

### Brief Description of the Interview:

#### [TO INTERVIEWER: PROVIDE THIS AS BACKGROUND TO INTERVIEWEE]

- The project is designed to help the APEC Business Advisory Council (ABAC) report to APEC Leaders on the impact of the new security environment on trade transaction costs.
- As part of this project, 14 USC students are spanning six APEC economies to interview port authorities, carriers, and exporting manufacturers and write Case Studies on their experiences with the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT) program, and the International Maritime Organisation's (IMO) International Ship and Port Facility Security Code (ISPS). We will be developing case studies from these interviews.
- The interview will take about 45 minutes.
- There are three parts to this interview:
  1. We will first ask you to assess your port's inspection capabilities and risk management strategies, etc. before the CSI and the new ISPS initiative was launched.
  2. We will then ask you to provide us with a description of how you went about complying with CSI and ISPS Standards and what type of technology you used in the process.
  3. Finally, we will ask you to give us your assessment of how CSI and the new ISPS is working (or not working for your port authority).

#### **CONFIDENTIALITY**

If you feel that there is any information that needs to be kept confidential, please do let us know during the interview and we will not disclose or caused to be disclosed this confidential information. If you wish, we will not disclose or caused to be disclosed your name or the name of your port. We will provide you with a copy of the case study to give you an opportunity to comment and make any changes that you feel are necessary.

#### **Part I: Assessment/Metrics on Old Regime:**

I would like to begin this interview by asking a few questions on the old security regime at your port.

1. How many tones of cargo did your port handle in 2004?
2. What were the major commodities and products handled by your port?
3. How much of this cargo was containerized?
4. How much of your container traffic was outbound to the United States?
5. Before your port became a CSI partner port, can you describe for me the capabilities of your customs administration in inspecting cargo outbound to the United States?

- a. Did your port use non-intrusive inspection equipment such as gamma- or X-ray imaging capabilities to inspect U.S.-bound cargo?
- b. Was there a risk management system in place to identify potentially high-risk containers? If so, can you describe what type of technology was used to identify and inspect high-risk containers?
- c. Did your port share critical data, intelligence, and risk management information with the United States Customs prior to CSI? If so, can you describe the extent of this liaison and the type of technology that was used to undertake sharing of data and intelligence?
- d. Did your port have an employee integrity program to identify and combat breaches of employee security? If so, can you describe how you would go about doing security checks prior to your port becoming a CSI partner?

## **PART II: Change Model and Processes put in Place to comply with CSI Standards**

I would now like to ask you questions on how your port went about complying with CSI Standards.

6. When and why did your port decide to become a CSI partner port?
7. What was the overall cost to your port of becoming a CSI partner port?  
**[Interviewer: Critical to get exact dollar values]**
8. What type of Non-Intrusive Inspection equipment did your port acquire?
  - a. How many x-ray or gamma-ray units did your port acquire and how much was the total capital outlay for the machines?  
**[Interviewer: Critical to get exact dollar values of capital outlay]**
  - b. How many operators needed training on the new x-ray or gamma-ray units and what is the total operating expenditure for the machines?  
**[Interviewer: Critical to get exact dollar values of operating expenditures]**
  - c. Were there any other investments related to x-ray or gamma-ray units (such as on-dock transportation machinery, creation of seclusion zones, warehouse, etc.) made by your port? If so, how much did these investments cost?  
**[Interviewer: Critical at this stage to try to separate out the cost associated with x-ray and gamma-ray machinery from the overall costs of complying with CSI]**
9. What type of automated risk management systems has your port put in place to identify high-risk containers?
  - a. How much was the total outlay (both capital and operational) for this risk management system?  
**[Interviewer: Critical to get exact dollar values of capital outlay]**

10. How does your port now liaise with U.S. Customs? What type of technology does your port authority deploy to share information with U.S. Customs? Were there any additional costs involved? If so, How much?
11. How does your port now address vulnerabilities in its infrastructure (fencing, patrols of perimeter, security cameras, etc.) due to changes in the ISPS code and the CSI initiative?
  - a. What type of technology did your port use to address these vulnerabilities?
  - b. How much did it cost to put in place the new security measures?
12. How does your port now undertake its employee integrity program? Is technology an important part of doing security checks on employees?

### **Part III: Assessment/Metrics on New Regime:**

I would now like to get your assessment of your ports experiences implementing CSI and ISPS, particularly some of the benefits and pain areas in complying with CSI and ISPS standards.

13. In your opinion, has CSI and ISPS resulted in increased export volume from your port?
14. In inspecting cargo outbound to the United States, have there been any delays as a direct or indirect result of the use of x-ray or gamma-ray machines?
  - a. What was the average transit time from port-gate to ship-hull before x-ray or gamma-ray machines were installed?
  - b. Have shipment times from port-gate to ship-hull increased, decreased, or remained the same after these machines were installed?  
**[Interviewer: If increase or decrease: What is the average time-release compared to before x-ray/gamma-ray installation?]**
15. What are the key pain areas in the use of technology that your port has experienced as a result of the CSI and ISPS initiatives?  
**[Interviewer: For example, have legitimate exports been quarantined because x-ray or gamma-ray machines have detected a false positive]**
16. In your opinion, have technological investments made by your port authority as a result of CSI and ISPS been beneficial to the movement of goods through your port?

## **Annex B: Interview Questionnaire for Customs Trade Partnership Against Terrorism**

### **[For Manufacturing Exporters]**

#### **Brief Description of the Interview:**

#### **[TO INTERVIEWER: PROVIDE THIS AS BACKGROUND TO INTERVIEWEE]**

- The project is designed to help the APEC Business Advisory Council (ABAC) report to APEC Leaders on the impact of the new security environment on trade transaction costs.
- As part of this project, 14 USC students are spanning six APEC economies to interview port authorities, carriers, and exporting manufacturers and write Case Studies on their experiences with the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) programs. We will be developing case studies from these interviews.
- The interview will take about 45 minutes.
- There are two parts to this interview:
  - a. We will first ask you to assess your firm's security programs and procedures before and after your firm **[became C-TPAT certified] [decided to become C-TPAT certified]**, how you went about complying with C-TPAT recommendations and what type of technology you used in the process.
  - b. We will then ask you to give us your assessment of how C-TPAT is working (or not working for your firm).

#### **CONFIDENTIALITY**

If you feel that there is any information that needs to be kept confidential, please do let us know during the interview and we will not disclose or caused to be disclosed this confidential information. If you wish, we will not disclose or caused to be disclosed your name or the name of your port. We will provide you with a copy of the case study to give you an opportunity to comment and make any changes that you feel are necessary.

---

I would like to begin this interview by asking a few questions about your firm and its interaction with your buyers in the United States.

- 1) What was your firm's world-wide annual gross revenue last year (in local currency)?
- 2) How much of your world-wide revenues were due to exports to the United States?
- 3) What products and/or services does your firm export to the United States?
- 4) How many employees does your firm have world-wide?

#### **Part I: Assessment/Metrics on Old and New Security Programs and Use of Technology:**

Now, I would like to ask a few questions on the old and new security program of your firm resulting from **[C-TPAT Certification]** **[preparing for C-TPAT Certification]**.

- 5) C-TPAT has a number of recommendations on Physical Security, Access Controls, Procedural security, and Personnel Security for exporting manufacturers. Did your firm make any changes to its existing security program to become C-TPAT certified? If yes, what was the overall cost to your firm of becoming C-TPAT certified?

**[If major costs were involved, proceed with the following]**

- 6) Before your firm **[became C-TPAT certified]** **[decided to become C-TPAT certified]**:
- A) Did your firm have to change locking devices for external and internal doors, windows, gates, and fences as a result of C-TPAT certification?
    - **[If yes]**, what type of new technology did your firm use to change these locking devices? How much did it cost?
  - B) Did your firm change external/internal communications systems to contact internal security personnel or local law enforcement?
    - **[If yes]**, what type of new technology did your firm use to change external/internal communication systems? How much did it cost?
  - C) Did any other physical security measures change for your firm as a result of C-TPAT certification?
    - **[If yes]**, can you describe these new security measures. How much did they cost?
- 7) C-TPAT has a number of recommendations on access control and tracking of employees, visitors and vendors. As a result of **[C-TPAT certification]** **[preparing for C-TPAT certification]** did your firm:
- A) Change how you identify, record and track employees, visitors, and vendors?
    - **[If yes]**, what type of new technology did your firm use to change this access control? How much did it cost?
- 8) C-TPAT has a number of recommendations on procedural security of incoming and outgoing goods. As a result of **[C-TPAT certification]** **[preparing for C-TPAT certification]** did your firm:
- A) Change how you record and track seals on containers, trailers and railcars?
    - **[If yes]**, what type of new technology did your firm use to change tracking of seals on containers? How much did it cost?
  - B) Change how you keep track of timely movement of incoming and outgoing goods?
    - **[If yes]**, what type of new technology did your firm use to track incoming and outgoing goods? How much did it cost?

- 9) Were there any other security measures undertaken by your firm? Please describe and identify how much these cost your firm.



**PART II: Assessment of C-TPAT**

I would now like to get your assessment of your firm's experiences **[implementing C-TPAT]** **[preparing for C-TPAT certification]**, particularly some of the benefits and pain areas in complying with C-TPAT recommendations.

- 10) In your opinion, has C-TPAT resulted in increased export volumes from your firm to the United States?
- 11) What are the key pain areas in the use of technology that your firm has experienced as a result of the C-TPAT initiative?
- 12) What are your overall opinion on C-TPAT and its impact on your firm's business?

**[For Sea and Air Carriers]**

**Brief Description of the Interview:**

**[TO INTERVIEWER: PROVIDE THIS AS BACKGROUND TO INTERVIEWEE]**

- The project is designed to help the APEC Business Advisory Council (ABAC) report to APEC Leaders on the impact of the new security environment on trade transaction costs.
- As part of this project, 14 USC students are spanning six APEC economies to interview port authorities, carriers, and exporting manufacturers and write Case Studies on their experiences with the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT) program, and the new International Ship and Port Facility Security Code by the International Maritime Organisation. We will be developing case studies from these interviews.
- The interview will take about 45 minutes.
- There are two parts to this interview:
  - a. We will first ask you to assess your firm's security programs and procedures before and after your firm **[became C-TPAT certified]** **[decided to become C-TPAT certified]**, how you went about complying with C-TPAT recommendations and what type of technology you used in the process.
  - b. We will then ask you to give us your assessment of how **C-TPAT** is working (or not working for your firm).

**CONFIDENTIALITY**

If you feel that there is any information that needs to be kept confidential, please do let us know during the interview and we will not disclose or caused to be disclosed this confidential information. If you wish, we will not disclose or caused to be disclosed your name or the name of your port. We will provide you with a copy of the case study to give you an opportunity to comment and make any changes that you feel are necessary.

---

I would like to begin this interview by asking a few questions about your firm and its interaction with your buyers in the United States.

- 1) What was your firm's world-wide annual gross revenue last year (in local currency)?
- 2) How much of your world-wide revenues were due to **[shipments]** **[passenger/cargo traffic]** to the United States?
- 3) How many employees does your firm have world-wide?

**Part I: Assessment/Metrics on Old and New Security Programs and Use of Technology:**

Now, I would like to ask a few questions on the old and new security program of your firm resulting from **[C-TPAT Certification]** **[preparing for C-TPAT Certification]**.

- 4) C-TPAT has a number of recommendations on Physical Security, Access Controls, Procedural security, and Personnel Security, Conveyance Security, and Manifest Procedures for sea carriers. Did your firm make any changes to its existing security program to become C-TPAT certified? If yes, what was the overall cost to your firm?

**[If major costs were involved, proceed with the following]**

- 5) Before your firm **[became C-TPAT certified]** **[decided to become C-TPAT certified]**:

- A) Did your firm have to change locking devices for external and internal doors, windows, gates, and fences at your warehouses and buildings?
- **[If yes]**, what type of new technology did your firm use to change these locking devices? How much did it cost?

- B) Did any other physical security measures change for your firm?

- **[If yes]**, can you describe these new security measures. How much did they cost?

- 6) C-TPAT has a number of recommendations on access control and tracking of employees, visitors and vendors. As a result of **[C-TPAT certification]** **[preparing for C-TPAT certification]** did your firm:

- A) Change how you identify, record and track employees, visitors, and vendors?

- **[If yes]**, what type of new technology did your firm use to change this access control? How much did it cost?

- 7) C-TPAT has a number of recommendations on procedural security for sea **[air]** carriers. As a result of **[C-TPAT certification]** **[preparing for C-TPAT certification]** did your firm:

- A) Change how you protect against unmanifested material being introduced into vessels operated by your company?

- **[If yes]**, what type of new technology did your firm use to protect against unmanifested material? How much did it cost?

- B) Change how you develop and provide information on crew and passenger lists?

- **[If yes]**, what type of new technology did your firm use to track legitimate crew and passengers? How much did it cost?

- 8) C-TPAT recommends that Manifests should be complete, legible, and accurate and need to be submitted in a timely manner. As a result of **[C-TPAT certification]** **[preparing for C-TPAT certification]** did your firm:

- A) Change how you develop and communicate your manifests internally and externally?

- **[If yes]**, what type of new technology did your firm use to communicate your manifests? How much did it cost?
- 9) C-TPAT also recommends that vessel integrity should be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security, according to C-TPAT should include the physical search of all readily accessible areas, the securing of all internal and external compartments, and procedures for reporting unmanifested cargo and tampering. As a result of **[C-TPAT certification]** **[preparing for C-TPAT certification]** did your firm:
- A) Change how you maintain vessel integrity?
- **[If yes]**, what type of new technology did your firm use to enhance vessel integrity? How much did it cost?

#### **PART II: Assessment of C-TPAT**

I would now like to get your assessment of your firm's experiences **[implementing C-TPAT]** **[preparing for C-TPAT certification]**, particularly some of the benefits and pain areas in complying with C-TPAT recommendations.

- 10) In your opinion, has C-TPAT resulted in increased trade volumes by your firm to the United States?
- 11) What are the key pain areas in the use of technology that your firm has experienced as a result of the C-TPAT initiative?
- 12) What are your overall opinion on C-TPAT and its impact on your firm's business?

## Endnotes

- <sup>i</sup> Janet Porter, 'US Customs to Defuse Bomb Threat', Lloyd's List Daily Commercial News, 24 January 2002, Internet archives:  
[http://www.lloydslistdcn.com.au/NASApp/cs/ContentServer?pagename=LLDCN/displayarticle&art\\_id=1010740392874&instance=1010740391859](http://www.lloydslistdcn.com.au/NASApp/cs/ContentServer?pagename=LLDCN/displayarticle&art_id=1010740392874&instance=1010740391859)
- <sup>ii</sup> US Customs Service, 'US Customs Container Security Initiative Guards America, Global Commerce from Terrorist Threat', press release, 1 November 2002 at: <http://parlinfoweb.aph.gov.au/piweb/repository1/media/pressrel/zeb960.pdf>
- <sup>iii</sup> We assume that at \$220/container and 15 million containers in circulation, the benefits of STAR-BEST could be extended to the entire global container fleet. See Bearing Point (2003). "APEC STAR-BEST Project Cost Benefit Analysis". November, 2003.
- <sup>iv</sup> See PECC. (2004). "Study on the Mutually Supportive Advancement of APEC's Trade Facilitation and Secure Trade Goals Post September 11". Pp. 44 – 48.
- <sup>v</sup> Anne McIlroy, "Container Boy sparks Terrorist Fears", The Guardian Unlimited.  
<<http://www.guardian.co.uk/elsewhere/journalist/story/0,7792,582851,00.html>>
- <sup>vi</sup> See Abt, Clark C. "The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability". Contract # DTRS57-03-P-80130. April 30, 2003. Cambridge, MA.
- <sup>vii</sup> In this section and in section 3.2., we have drawn heavily from the US Customs and Border Protection website. For details, see: [http://www.customs.gov/xp/cgov/border\\_security/international\\_activities/csi/](http://www.customs.gov/xp/cgov/border_security/international_activities/csi/) and [http://www.customs.gov/xp/cgov/import/commercial\\_enforcement/ctpat/](http://www.customs.gov/xp/cgov/import/commercial_enforcement/ctpat/)
- <sup>viii</sup> See "Statement by Senator Carl Levin (D-Mich) before the Permanent Subcommittee on Investigations. May 26, 2005.
- <sup>ix</sup> See OECD. (2003). "Security in Maritime Transport: Risk Factors and Economic Impact." Maritime Transport Committee of the OECD: Paris, pp. 3.
- <sup>x</sup> We assume that at \$220/container and 15 million containers in circulation, the benefits of STAR-BEST could be extended to the entire global container fleet. See Bearing Point (2003). "APEC STAR-BEST Project Cost Benefit Analysis". November, 2003.
- <sup>xi</sup> See OECD. (2003). "Security in Maritime Transport: Risk Factors and Economic Impact." Maritime Transport Committee of the OECD: Paris, pp. 18.
- <sup>xii</sup> See "Supply Chain Sustainability and Cost in the New War Economy." *Traffic World*, April 1, 2002.