Smart Containers and the Public Goods Approach to Supply Chain Security

Dr. Darren Prokop

Department of Logistics
College of Business & Public Policy
University of Alaska Anchorage

Business Education Building
3211 Providence Drive
Anchorage, Alaska
99508
tel. 907-786-1992
fax. 907-786-4115
e-mail: afdjp1@cbpp.uaa.alaska.edu
website: http://logistics.alaska.edu

Introduction

Robert Bonner, former Commissioner, U.S. Customs and Border Protection wondered: "When you open your refrigerator door, a light lights up. I don't know why we can't do that with a container." (**Traffic World 2004; p. 19**).

After providing a brief history of containerization this paper will: review the state of technology related to smart containers; discuss their role in the drive to secure global supply chains; and add clarity to strategic decisions faced by government, shippers and carriers by way of the economics of public goods.

The Smart Container and the "Green Lane" Benefit

The United States Bureau of Customs and Border Protection (CBP), under the Department of Homeland Security (DHS), has offered to give "green lane" treatment to any smart container arriving at a port of entry. What is required is the inbound container was: (1) cleared through a foreign port under the Container Security Initiative (CSI); and (2) is being used by shippers and carriers who are members of, and compliant with, Customs-Trade Partnership Against Terrorism (C-TPAT).[1] Promised benefits--- of this so-called C-TPAT-Plus--- would be no inspection and immediate release at the port of U.S. entry. The problem is that there is no smart container currently in use; nor is the nature of a smart container yet agreed to by industry and government. If compliance is possible there are some benefits. CBP estimates that one in 47 of a company's inbound shipments are pulled for inspection as compared to one in 306 if C-TPAT compliant.[2] Presumably, C-TPAT-Plus would see no shipments pulled. The problem though is the calculation of *net* benefits or the return on investment from C-TPAT-Plus.

A U.S. importer who is a member of C-TPAT must sign a memorandum of understanding with CBP in which it prepares a security plan and ensures its viability through a comprehensive self-assessment. Some of the membership criteria are:

(1) verify security practices of international supply chain partners;
(2) maintain container and/or vehicle security;
(3) control employee and visitor access to facilities;
(4) perform criminal background checks on employees;
(5) secure both physical and information technology assets

Point (1) is supposed to be achieved by using leverage in the contracting process to ensure a trickle down effect of C-TPAT standards upstream along the supply chain.

The problem for CBP is that it has decided to validate the international supply chains of C-TPAT members. And this is to take place over many countries and foreign vendors. Would it be willing to outsource this process to private companies if CBP inspectors are not allowed to perform on-site visits in the country in question? For example, it is private accountants and lawyers who prepare tax returns, not the Internal Revenue Service. At present outsourcing does not appear likely.[3] Of course, outsourced or not there will be problems in verifying, say, a plant in China with a transient labor force or countries with privacy laws which forbid background checks along the lines envisioned by CBP. But if the U.S. importer has enough leverage over its partners along its international supply chain, C-TPAT is *de facto* pushing supply chain security beyond U.S. ports of entry which is a plus.

The standards CBP are looking for in security plans involve: selecting vendors; physical access controls; personnel; document compliance; training; conveyance security; and protection of information technology. According to CBP, Tier 1 shippers are those in C-TPAT; Tier 2 are those whose import security plans are under audit; and Tier 3 are those who are deemed C-TPAT-Plus and entitled to "green lane" benefits.

As far back as October 2003, CBP initially wanted to make container door sensors part of the requirements for C-TPAT. Of course, this never came about because of the unreliability of the technology then and at present. CBP, when referring to a smart container, has no specific device in mind. Alternatives undergoing examination are:

(1) An e-seal which is an active radio frequency identification (RFID) tag attached to the mechanical seal on the outside of the container. Active tags have their own power source unlike the more prevalent (and inexpensive) passive tags used in inventory control;

(2) A tamper-alert device to be permanently installed inside the container as opposed to temporarily on the door (which itself could be removed and reattached after any malfeasance);

(3) A global positioning system (GPS) for container tracking and cargo status updates.

The active tag is a device providing a tracking option; it does not signal malfeasance. These tags are being developed by Savi Technology. The tamper-alert device, on the other hand, is being developed by General Electric (GE) under the name "CommerceGuard". Both companies are, needless to say, in competition with each other.[4] Each, however, may benefit from research grants provided under Operation Safe Commerce (as run by DHS' Border and Transportation Security Directorate). The ideal device may be described as reliable and having: multiple sensors; wireless communication; and an ability to detect both breaches on the outside of the container and specific changes to its contents on the inside. Of course, any device is practically useless unless the in-coming data is properly leveraged by a well-crafted management system. If not, RFID and tamper-alert devices are just expensive bar codes.

Since CBP does not have the resources to interdict a container every time an alarm is sounded, it is looking for a device with false alarms at a rate of less than one percent. Note that 30 false alarms on a vessel with, say, 3,000 containers can be a nuisance to the port operators. Among the devices in development at present the false positives are around five percent.[5] And door seal compromises appear to be the most realistic item for detection at this time. CBP, however, has an ambitious list of items it wants scrutinized. These would involve changes in: light, temperature, motion, weight, air pressure, radiation, chemicals, and biological agents. The problem is that the more sensitive the device becomes the more apt it may be to false alarms because of the daily moving and jarring which containers receive.

Of course, the container itself should not be the entire focus of emerging technology. The ports of entry also have a role to play. The standard radiation detectors deployed at several U.S. ports cannot detect radiation if a nuclear device were shielded with dense lead or steel. Gamma ray detectors, however, would be able to overcome that problem.

In December 2005, the Commercial Operations Advisory Committee (COAC), which advises CBP on industry points of view, recommended a series of benefits for the "green lane" which may be summarized as follows:

(1) Expedited duty drawback;
(2) No penalties for late duty payments;
(3) Remote electronic filing of all CBP entries (i.e., no need to file at actual port of entry);
(4) No inspections at entry unless criminal activity is suspected;
(5) Expedited CBP rulings in case of a dispute (i.e., 10 days vs. 30 days);
(6) Expedited employee background checks

Containerization: A Brief History

Malcolm McLean, founder of Sea-land Service, is generally considered to be the father of containerization. His revelation came when he watched dock workers unloading cotton off of truck trailers only to reload them onto an ocean vessel. McLean thought it would be so much easier just to hoist the trailer itself onto the deck of the vessel and save multiple dollars and hours in the process.

To make his idea more practical McLean devised a thirty-five foot steel container which could fit on a trailer frame and be stacked in the hold of an ocean vessel. Using a newly-purchased (and converted) steam ship, the Ideal X with 61 trailers lashed to the deck, the first containerized voyage from Newark to Houston took place on April 26, 1956. Fifty-eight containers were aboard. Since that maiden voyage containers grew in popularity with their sizes and fitting becoming standardized so that they could be fitted onto any other container, trailer chassis, ocean vessel, flatbed rail car, or cargo airplane belly.

This new reality, intermodalism, gave rise to efficiency gains since the container was simply transferred among various conveyances without having to be opened. But this hands-off approach also presents an opportunity for foul play since the container's contents were assumed to be uncompromised after the container doors were closed at the point of origin. In this vein it now makes sense to account for container security by affixing: a tamper proof seal; tracking device; or internal device to the container on its journey from origin to final destination.

Container Security Steps: Post 9-11

The ideal for CBP is to know when, where and by whom a container changes hands along the supply chain. CBP has a five-point agenda for container security. These are:

(1) C-TPAT (Still Voluntary)
(2) Container Security Initiative (CSI) (the goal is 50 ports by 2007)
(3) Advance Manifests (e.g., the so-called 24-Hour Rule for ocean vessels)
(4) Non-electronic Container Seals
(5) Smart Containers (as part of C-TPAT-Plus) in Full Use

Points (3), (4) and (5) are still in the implementation stage.

Currently, CSI ports account for 75% of the global origins of U.S. bound containers. In Europe CSI accounts for 84% of U.S. inbound containers. Similarly, CSI ports in Asia account for 90% of U.S. inbound containers. At CSI ports CBP inspectors will screen (as opposed to physically inspect) all U.S. bound containers based on the documents received from the carrier.

Table 1: Ports in the Container Security Initiative

Continent/ Region	Country	Port
North America	Canada	Halifax, Montreal, and Vancouver
Europe	Belgium	Antwerp and Zeebrugge
	France	Le Havre and Marseille
	Germany	Bremerhaven and Hamburg
	Greece	Piraeus
	Italy	Genoa, Gioia Tauro, La Spezia, Livorno and Naples
	Portugal	Lisbon
	The Netherlands	Rotterdam
	Sweden	Gothenburg
	Spain	Algeciras
	United Kingdom	Felixstowe, Liverpool, Thamesport, Tilbury and Southampton
Asia	China	Hong Kong, Shanghai and Shenzhen
	Japan	Kobe, Nagoya, Tokyo and Yokohama
	Malaysia	Port Klang and Tanjung Pelepas
	Singapore	Singapore
	South Korea	Pusan
	Sri Lanka	Colombo
	Taiwan	Kaohsiung
	Thailand	Laem Chabang

Table 1 (Cont.):

Continent/Region	Country	Port
Middle East	**United Arab Emirates**	**Dubai**
	Oman	**Salalah**
Africa	**South Africa**	**Durbin**
South America	**Argentina**	**Buenos Aires**
	Brazil	**Santos**

After the screening the container is loaded onto the vessel; and it may be pulled for physical inspection at the U.S. port of entry based on a risk assessment carried out while in-transit. About 6% of inbound containers are physically inspected. To date the 43 ports that have agreed to accept CBP inspectors as part of CSI are shown in table 1.

Since CBP is not interested in outsourcing the C-TPAT compliance process along the international supply chain it is the case that any points at or near CSI ports have a comparative compliance advantage over those which are not.[6]

Advance manifests, submitted to CBP by the carriers, are a requirement under the *Trade Act* of 2002. Currently, electronic manifests are filed by the ocean vessel, rail and air modes via Customs Automated Commercial System (ACS). Motor carriers, on the other hand, file via their customs brokers (who use the Automated Broker Interface (ABI)). The newly anticipated Automated Commercial Environment (ACE) will allow motor carriers to file directly (thus complying with the *Trade Act*). As of January 31, 2005 ACE has being tested at the Blaine, WA border crossing.[7] The challenge of connecting ACE to the legacy systems in use has been the reason why the motor carrier mode has lagged behind.

Currently, the compliance process for container seals are as follows. CBP announced in September 2004 that non-electronic seals need to be placed on all U.S. inbound containers (a flow of about 9.5 million per year). There is no compliance deadline as yet. Worldwide, containers number about 19 million with any one of which possibly finding its way into the U.S. These seals are simply to be manually inspected along the supply chain for evidence of tampering. If a scanning device at the port of entry is not available and the container is marked for physical inspection CBP, as of August 2005, will seal the containers with ISO-standard seals having unique serial numbers. In the past there was no standard seal in use.

The progression from seals to smart containers may be characterized as learning to walk before learning to run. As such, the "green lane" is reserved for electronic security technology of some sort on the containers. At a minimum this would involve active RFID tags which would provide pertinent tracking and content information. As noted above, however, an effective electronic security device is still being worked out.

Smart Containers: A Public Goods Analysis

Essentially, a smart container is a physical and electronic technology combined with a conveyance and is used by both the shipper and the carrier. With the exporter loading it and the carrier transporting it overseas to the U.S. importer the smart container is an item common to all players and, therefore, is easier to build into a consistent and homogenous international supply chain security plan. There is also greater incentive for cooperation in the game-theoretic framework which characterizes the compliance process (***q.v.*, Prokop 2004**). With an indivisible item such as a smart container the voluntary provision of supply chain security--- in the context of what economists refer to as a public good--- can be analyzed.

Under voluntary provision of a public good the firm (i) treats it like any other factor of production. Its desired provision of security (S_i) along a portion of the firm's supply chain leads to overall supply chain security of ($\Sigma_i S_i$) where each provision need not be equal over all (i). The firm's production function of the final good (Y) along a supply chain is based on the usage of a standard input (X) and the public good (S_i) which is subject to a budget constraint[8]:

$$\text{max. } Y_i(X_i , S)\text{; subject to: } TC_i = P_x X_i + P_S S_i$$

The result is the familiar marginal rate of technical substitution (MRTS) of the standard input for the public good (*qua* input) equaling the ratio of input costs:

$$[(\delta Y_i/\delta S) / (\delta Y_i/\delta X_i)] = (P_S/P_X) \tag{1}$$

Equation (1) may be referred to as a Cournot-Nash (CN) solution. For a Pareto-optimal (PO) solution, however, some consideration must be given to all firms within the supply chain. Following **Samuelson (1954)** a social welfare function (W) over all Y_i has to be maximized subject to an aggregate budget constraint. Assuming a utilitarian (additive) W for simplicity, we have:

$$\text{max. } W = \alpha_1 Y_1 + \alpha_2 Y_2 + \cdots + \alpha_n Y_n \ ; \ \alpha_i > 0$$

$$\text{subject to: } \Sigma_i \, TC_i = P_x \Sigma_i \, X_i + P_S S$$

The result is:

$$\Sigma_i \, [(\delta Y_i/\delta S) / (\delta Y_i/\delta X_i)] = (P_S/P_X) \tag{2}$$

The difference between equations (1) and (2) indicates that Pareto-optimality requires the summed $MRTS_i$ to equal the price ratio. But it is also the case that S_i is not as large under voluntary provision. To see this, equation (2) may be rewritten with firm (i) isolated:

$$[(\delta Y_i/\delta S) / (\delta Y_i/\delta X_i)] = (P_S/P_X) - \Sigma_j \, [(\delta Y_j/\delta S) / (\delta Y_j/\delta X_j)] \tag{3}$$

The second term on the right hand side of equation (3) is greater than zero so long as negative returns are ruled out over S and X.[9] If so, then for firm (i):

$MRTS^{CN} > MRTS^{PO}$; so for a given MPP_X we have $MPP_S^{CN} > MPP_S^{PO}$

Since optimality occurs in the range of diminishing returns to the inputs, too little S is provided under CN than under the social welfare maximizing PO. For PO to occur an external coordinating mechanism (i.e., the government) is necessary to coordinate all expenditures on S across the firms along the supply chain.

Now suppose the effective provision of S requires a team effort. Instead of an additive function, S would only be as good as the weakest link (**Hirshleifer 1983**). In that case, $(\delta S/\delta S_i)=0$ when $S_i>S_j$ for some j. The provision of S could be written as:

$$S = S_1 + wS_2 + \cdots + wS_n \text{ ; where } (0 \leq S_1 \leq S_{2\ldots n}) \text{ and } (0 \leq w \leq 1) \quad (4)$$

According to equation (4) $S=S_1$ when w=0 and the smallest contributor (i.e., firm 1 as the weakest link) determines effective and overall supply chain security. Any effective breach of security would be centered on firm 1 such that all other contributors cannot add to security. At the other extreme, S is additive across all contributors when w=1. Any effective breach would not be attributable to any one firm. In fact, effective breaches would be random and inversely proportional to the mean level of S_i across all i. In the intermediate case, as (w) grows from zero to one the more firms 2 through n determine the effective level of S.

Using equation (4) as a guide, consider a simple two-firm supply chain (say, a U.S. importer and a foreign vendor). If the importer is C-TPAT compliant then if one of the two firms were to be a weak link it would be the foreign vendor. The solution for firm 1 (the vendor) is represented by equation (1). But for firm 2 (the U.S. importer) it becomes[10]:

$$[(\delta Y_2/\delta S) / (\delta Y_2/\delta X_2)] = [(P_S/w) / P_X] \quad (5)$$

Firm 2 faces a higher relative price for S and would, therefore, volunteer to purchase less of it than firm 1 which violates the conditions on equation (4). For that to occur, however, firm 2 would have to know the technology leading to equation (4) across the supply chain. But if it is not known the firm will over-provide S_2. As (w) falls this effect becomes more pronounced because, when w=0, it would only make sense for firm 2 to provide an S_2 equal to that of the weak link. The degree to which firm 2 can leverage its knowledge of firm 1 and alternative vendors will determine how successful it would be in working with a state of supply chain security (as given by equation 4) which would have (w) at a level suitable for firm 2 to pass a C-TPAT audit.

The Pareto-optimal result is found by choosing a level of X_1, X_2 and S which maximizes Y_1 (with Y_2 held constant) subject to equation (4). The solution is:

$$[(\delta Y_1/\delta S) / (\delta Y_1/\delta X_1)] + w\, [(\delta Y_2/\delta S) / (\delta Y_2/\delta X_2)] = (P_S/P_X) \qquad (6)$$

With w=1 equation (6) is identical to equation (2) and the firms, acting independently, will each purchase too little S_i. And with w=0, firm 1 is the weakest link and its provision of S_1 becomes optimal since no other firm can add to that level of performance. In that case equation (6) is identical to equation (1) and the CN solution merges with the PO. Firm 2 would match S_1 and this is the only situation where firms acting independently are able to achieve a Pareto-optimal result without the need for government coordination.

What of the carrier? In a three firm supply chain the C-TPAT importer would prefer to deal with a carrier using CSI ports of exit. Surely, the foreign vendor would remain the weakest link in this chain. Indeed, the carrier may have to put pressure on the foreign vendor to provide the necessary paperwork the carrier needs to provide to CBP personnel stationed at the CSI port.

In summary, as (w) and/or the number of firms along the chain increases the more S diverges from PO and the greater is the degree of under-provision of security by the firms. With CBP only able to regulate shippers and carriers making contact with U.S. territory it is easy to envision overseas firms as the weak link under the C-TPAT audit. Of course, regulating the U.S. importer and the U.S. inbound carrier makes sense as they may be able to use their own leverage in the contracting process to mitigate any weak links (i.e., raise the value of (w) across the supply chain).

On the issue of weak links consider the confusion related to non-electronic seals. While the importers understand that it is they who are mandated under C-TPAT to develop the supply chain security plan it was not clear who was responsible for affixing the container seal and maintaining records as to breaches *en route*. Consider the vendor-exporter in a foreign country. Is the onus on the U.S. importer to ensure that the foreign-based vendor complies with this detail of C-TPAT; or should it be the carrier who is in physical contact with the vendor? If the carrier is C-TPAT compliant would it wish to take that responsibility? Furthermore, suppose there were a third party logistics provider (3PL) in between the importer and the carrier? CBP has mandated the U.S. importer as ultimately responsible through its submitted plan.

It makes sense that the U.S. importer is the first-mover in this process and so, therefore, should expend the most leverage in making sure its supply chain maintains C-TPAT compliance. The importer must verify that its partners are either C-TPAT members or, if not, they are meeting the baseline criteria for C-TPAT. In any case, non-U.S. parties have the incentive to free ride.

C-TPAT is voluntary and subject to CBP compliance. This means the program is at once flexible to the uniqueness of each company's supply chain and yet overseen by a regulatory bureau's desire for uniformity. Is it workable? All the risk seems to be borne by the U.S. importer who also lives under the threat of removal from the program without notice.

Apart from the voluntary C-TPAT program, the advance manifest requirement for ocean carriers is not. Since 2003 ocean carriers have adjusted to the "24 Hour Rule". CBP's risk assessment regarding the container, therefore, is based on information handled by the carrier and not the importer. In other words, the importer may be the first-mover in the supply chain; but it is the carrier who is the first-mover in the compliance process regarding the container. Why? One of the items required in an e-manifest is information regarding the exporter (consignor) and U.S. importer (consignee) (**Prokop 2004; tab. 3**). But those details rest with how much information the carrier is able to obtain. The contact information for the exporter is useful but where was the goods' point of origin and where was the container packed? Thus, data are submitted at the time the carrier takes charge of the container; not at the foreign factory, warehouse or distribution center. This is an unavoidable hole in the compliance chain.

The carrier will be squeezed on two sides to adopt a smart container. On the one side is onus it has from CBP to comply with CSI; on the other is the C-TPAT shipper who will demand a carrier use a smart container and add weight to the shipper's audit for green lane benefits.

Conclusions

Since smart container technology (and the green lane benefit) is some ways into the future C-TPAT may be looked upon as an insurance policy. If U.S. ports of entry were shut down it is C-TPAT freight which would move first when the ports were reopened. Importantly, the CBP's green lane could be overridden by the Food and Drug Administration (FDA) or the Department of Agriculture which operate within different stovepipes. Should a shipment involve trade regulations beyond those handled by CBP there is no guarantee for green lane benefits.

Some in the industry have asked about the cost of compliance in order to achieve a truly smart container. Because RFID tags and security technology are merely a cost overlay, the bigger question is how the business process should change in the face of the new data gathered. Turning the data into knowledge is the challenge. Rather than cost the better measure is the net benefit (if any) to be derived from the data, the security "visibility", and the green lane.

Endnotes

[1] CBP's counterpart for domestic cargo security is the Transportation Security Administration (TSA). On the foreign front, Customs-Trade Partnership Against Terrorism is a voluntary program. Shippers and carriers who join are deemed to be "low-risk" and are required to accumulate data in order to report to CBP on a monthly basis (when appropriate customs duties are to be assessed). In the motor carrier sector, for example, a shipment from Canada or Mexico would be preceded to the border by an electronic transmission to customs officials. The driver simply presents bar codes at the border which are scanned and then he is waived through. Of course, the motor carrier and all shippers, represented by the container's contents, must be in a special part of C-TPAT (known as Free and Secure Trade, FAST) to avoid the standard routine of inspection. By 2007, FAST (non-FAST) carriers entering the U.S. must submit their e-manifests 30 minutes (1 hour) before actual arrival at the border. As of January 2006 over 10,374 companies applied for C-TPAT membership. Because of the lengthy time involved in the vetting process 5,727 have been accepted thus far and, of these, 1,400 have had their security plans validated by CBP. Validation is handled through on-site visits.

[2] These estimates were provided by former CBP Commissioner, Robert Bonner (**Kulisch 2005; p. 30**).

[3] According to Todd Owen, C-TPAT Director: "A big part of C-TPAT was trust and the partnership that's being developed between the government and the company. If we bring in third parties, it would not be as effective as the way we're doing it now." (**Edmonson 2005; p. 15**).

[4] GE's device is similar to RFID but uses proprietary technology independent of the ISO 17712 standard for transoceanic container seals which covers tensile strength, sheer, bend and impact for non-electronic container seals. The sensor (which has a 10-year battery life) detects and records when the door is opened. Furthermore, at ports, railheads, or wherever the reader is placed, a

short wave signal indicating tampering could be received. Typical containers have an operating life of about 10 years as well. By way of comparison RFID e-seals cost up to $20/unit while GE's "CommerceGuard" is estimated to be $1,000/unit.

[5] False positives can be expensive. For example, the Palermo Senator ocean vessel was delayed for three days off of the Port of New York in 2002 because of harmless radiation emitted from some clay tiles. Over two thousand other containers were delayed entry as a result. The GE device was recently tested in selected trade lanes by CBP and came up with a false positive rate of only 0.3%. But the electronic date and time stamps for the events had failure rates of about 4% due to malfunctions of the internal clocks (**American Shipper Online**). Thus, there appears to be some potential for CBP compliance.

[6] Private sector proposals for supply chain security standards are occurring beyond the United States. Most prominent is the proposed ISO 28001 "Best Practices for Custody in Supply Chain Security". Outside auditors would vet the compliance process rather than customs inspectors. While CBP has no problem with ISO standards on equipment (e.g., physical and electronic seals) it does have problems with the independent establishment of process standards.

[7] While ACE is to be rolled out incrementally at Canadian and Mexican border crossings, motor carriers currently use two systems to communicate with border officials: the Pre-Arrival Processing System (PAPS) and Border Release Advance Screening and Selectivity (BRASS). Basically, low-risk, high-volume freight from pre-approved shippers is pre-screened by CBP officials in Canada or Mexico before arriving at the border. As of May 1, 2005 all BRASS carriers must be FAST-compliant as well.

[8] The production process in this context includes the relevant logistics of international shipping and customs clearance.

[9] In fact, this second term becomes larger when: (1) the amount firm (i) thinks all other firms (j) are spending on S goes up; and (2) the number of firms along the supply chain goes up. In the traditional approach to public goods analysis, S and X would be final goods and the parallel condition is that S and X be normal goods in their utility functions.

[10] The Lagrangian leading to equation (5) requires $S_2 = (S/w) – (S_1/w)$.

References

American Shipper Online. (2006). “Smart box tests show low false alarm rates; other problems crop up.” Jan. 20.

Edmonson, R. (2005). “Green Lane in Sight.” *The Journal of Commerce*. Jan. 24. p. 15.

Hirshleifer, J. (1983). “From Weakest-Link to Best-Shot: The Voluntary Provision of Public Goods.” *Public Choice*. vol. 41. no. 3. pp 371-86.

Kulisch, E. (2005). “Congress puts C-TPAT, CSI under Microscope.” *American Shipper*. July. pp. 30-8.

Prokop, D. (2004). “Smart and Safe Borders: The Logistics of Inbound Cargo Security.” *International Journal of Logistics Management*. vol. 15. no. 2. pp. 65-75.

Samuelson, P. (1954). “The Pure Theory of Public Expenditure.” *Review of Economics and Statistics*. vol. 36. pp. 387-89.

Traffic World. (2004). Dec. 20/27. p. 19.