



Asia-Pacific
Economic Cooperation

2007/ASCC/1.5

Session: Secure Trade – The Impact of Terrorism

1.5.3

Challenges for Customs

Purpose: Information

Submitted by: Adj Prof Mark Harrison

Centre for Customs and Excise Studies, University of Canberra



**Annual Conference of APEC Centres
Melbourne, Australia
18-20 April 2007**

Customs and Supply Chain Security - “The Demise of Risk Management?”

Mark Harrison and Steve Holloway

Contemplate this: Over 200 million containers are being shipped between countries annually yet only about 2% of those containers are physically inspected¹. In some countries the percentage physically inspected may be higher but we are still generally talking about single digit percentages². Now inject into that traffic a single container that in a false partition hides nuclear material or a biological pathogen. What is the chance that Customs will detect the illicit cargo? How likely is it that that container will make its way into the domestic commerce of the targeted country? This is the nightmare scenario that Customs has confronted since 9/11 and a variation on a theme that has operated since trade first began.

What is being done to manage the risks associated with the new security environment? There can be no doubt that the regulation of international trade has increased markedly in the period since 2001 and that customs administrations have been at the heart of those regulatory changes. This increase in regulation has occurred both nationally and internationally with key and can I suggest benchmark supply chain security initiatives originating (unsurprisingly) in the United States.

It is worthwhile considering the US and international initiatives for a moment before making some observations and drawing some conclusions on the intersection between customs administration and supply chain security. These initiatives include:

- The US Advanced Manifest Rule requiring detailed cargo data to be submitted to US Customs and Border Protection prior to arrival. A sea container is only allowed into the United States if detailed information about its contents has been submitted electronically to Customs at least 24 hours prior to loading on board the ship at the port of origin.
- The US Container Security Initiative (CSI) which pushes inspections and screening upstream to originating ports. CSI has focussed on the twenty ports where most of the US-bound containers originate. It relies on a series of bilateral agreements that permits exchange of Customs officers and more screening of shipments at the outbound ports.
- The US Customs-Trade Partnership Against Terrorism (C-TPAT) which is a voluntary program that provides certain benefits, such as reduced inspections, to companies that can show that they meet a minimum level of supply chain security. The higher the level of compliance with supply chain security as judged by CBP auditors the more benefits that are intended to flow. There are three tiers of C-TPAT compliance, with the intention that those companies at the third tier have their cargo flow virtually unimpeded across the border.
- The US Free and Secure Trade (FAST) initiative allows low-risk goods transported by trusted drivers via trusted carriers for trusted firms to pass rapidly through border

¹ Closs, David J; McGarrell, Edmund (2004), “Enhancing Security Throughout the Supply Chain,” IBM Center for Business of Government, April 2004

² As of 2004 only 6% of the containers imported to the US were physically inspected – US Customs and Border Protection website (2004), “Cargo Container Security – US Customs and Border Protection Reality,” October 2004. In Australia that figure is closer to 7% - Australian Customs Service website, October 2005

crossings while allowing Customs inspection resources to concentrate on unknown or high-risk shipments.

- The US Smart and Secure Trade-Lanes (SST) program provides a complete audit trail of a container's journey from origin to final destination utilizing the world's three largest seaport operators – Hutchison-Whampoa Ltd, PSA Corporation Ltd, and P&O Ports – representing over 70% of the world's container traffic.³
- The ISO/PAS 28000:2005 standard, 'Specification for security management systems for the supply chain' by the ISO, which outlines the requirements for an organization to establish, implement, maintain and improve a security management system, including financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations.⁴
- The World Customs Organization (WCO) has been developing standard sets of customs data elements to enable advanced electronic transmission of such data consistent with the push by various customs administrations for advance transmission of data prior to the arrival of goods. The WCO has also developed a Framework of Standards to Secure and Facilitate Global Trade, known in shorthand as the SAFE Framework. As of June last year, a total of 135 countries had expressed their intention to implement the WCO SAFE Framework, including 25 member states in the European Union.⁵
- Within APEC, at the second meeting of the Sub-Committee on Customs Procedures in 2005, members adopted the APEC Framework for Secure Trade, based on the WCO SAFE Framework. A key element is voluntary partnerships established between customs administrations and businesses operating in the import/export environment. These partnerships are known as Authorised Economic Operator (AEO) programs, and aim to strengthen the security controls over the handling, transport and storage of cargo while providing benefits to industry partners who can demonstrate required levels of security along their supply chains.
- Within the EU, as from 1 January 2008 the AEO concept is introduced and from July 2009 it will become mandatory for traders to provide customs authorities with advance information on goods brought into, or out of the customs territory of the European Community. Failure to do so will mean goods cannot be loaded on ships bound for the EU.

It is self-evident that there is and has been a multiplicity of policy and standard-setting activity by governments and international organizations in relation to supply chain security and the way in which customs administrations acquit their border responsibilities. The United States has led the charge in this regard and their initiatives have had a significant impact on both regulatory change in other countries and the manner in which companies engaged in international trade manage their supply chains. The fact is that the United States remains a key and perhaps principal export market for many countries and if they wish to continue to trade with the US they must be aware of and implement US supply chain security measures.

³ Hudson, Scott (2006), "Smart and Secure Tradelanes (SST), Supply Chain Resource Consortium, February 21, 2006 <http://scm.ncsu.edu/public/security/sec060221.html>. In May 2003, the ISO formally became involved with the SST program with a view to the establishment of international supply chain security and visibility standards

⁴ <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=41921>

⁵ WCO Website, <http://www.wcoomd.org/ie/En/en.html>, under "List of Members who have indicated their intention to implement the SAFE Framework of Standards."

While there has been a hive of regulatory activity nationally and internationally there are also an increasing number of “pilot” programs being conducted by countries to apply the SAFE Framework to existing trade and to test AEO concepts with a view to achieving mutual recognition of individual programs between trading partners. Therefore the EU and China are conducting a pilot program and Australian Customs is conducting an AEO pilot program with the United States, Singapore and New Zealand under the auspices of APEC.

With respect to Australia’s “Supply Chain Security Pilot” there are two published objectives:

- The testing and fine-tuning of application and assessment processes for security accreditation of importers, exporters and others in the supply chain; and
- Reaching agreement on mutual recognition from other customs administrations involved in the pilot⁶

So what does all of this mean in a practical sense for both customs administrations and companies engaged in international trade?

The most immediate observation that can be made is that Customs role as the ‘protector of the border’ has become pre-eminent, possibly to the detriment of its revenue and commercial compliance roles. This is most starkly reflected in the United States where “Customs and Border Protection” form a key part of the Department of Homeland Security and it has certainly been the subject of vigorous policy debate within the Australian political scene. The historical fact is that Customs was originally created to enforce tariffs and calculate import taxes and while that role expanded to combat drug trafficking, regulating trade was its traditional role. Now, to quote Robert Bonner, the former Commissioner of US Customs and Border Protection “The priority mission of US Customs is national security” and an increasing number of customs administrations feel the same way.

‘Counter-terrorism’ and ‘weapons of mass destruction’ have well and truly overtaken the more mundane customs terms of ‘tariffs’, ‘revenue compliance’ and even “drug interdiction’ in the Customs lexicon. The notion of trade facilitation still exists but more often than not it is used in the same sentence as “....while protecting the security of the supply chain”.

Of course this change in the Customs dynamic is not unreasonable given the potential impact of a terrorist or other incident on global supply chains. For example, an October 2002 war game that mimicked such a scenario found that closing US ports for as many as 12 days created a 60-day container backlog and cost the economy approximately \$58 billion.⁷ However, another quote is equally thought-provoking: “The goal of terrorist events is to bring our economy to a standstill. If we put an anti-terrorist mindset on and make the protocol extremely cumbersome to avoid the terrorist event, we risk achieving the same outcome the terrorists desire”.⁸

⁶ See www.customs.gov.au under APEC 2007

⁷ Quoted in “Customs Rattles the Supply Chain”, March 1, 2006 edition of CIO Magazine

⁸ Mr Stephen Zujkowski, Senior Vice-President, Savi Technology cited in Hannon, D (2002). High-tech security becomes top priority in supply chain. Purchasing Magazine (June 2002)

Has the new emphasis on supply chain security therefore altered customs philosophy on achieving a balance between customs control and trade facilitation? This question is not entirely rhetoric. If I can address it by reference to three themes:

1. Risk management;
2. The relationship between customs and industry, and
3. Information management

Risk management has always been at the core of customs administration and is a fundamental discipline enshrined within the WCO's Revised Kyoto Convention on the Simplification and Harmonization of Customs Procedures. It has proven to be the most effective means of managing the huge volumes of cargo that enter the country every day of the week because it allows an administration to concentrate resources on areas of high-risk while allowing low-risk cargo to flow unimpeded into the commerce of the country. In short, risk management coupled with good intelligence and effective data analysis allows the profiling and targeting of cargo prior to arrival at a port so that low-risk cargo can be released immediately and high-risk cargo can be diverted for physical examination.

On its face, one could be forgiven for adopting the view that the lower tolerance for risk associated with the new security environment has led to the demise of risk management in favour of zero tolerance and 100% inspection. Indeed after 9/11 there were calls from some quarters for the inspection of each and every container entering the country. However, the fact remains that "the vast majority of containers are filled with legitimate goods from legitimate sources heading to legitimate companies"⁹ and this has maintained the utility of risk management for supply chain security.

In other words while the nature of the risk equation has changed the still increasing volumes of trade has meant retention of risk management as the most effective methodology for facilitating trade and achieving security of the supply chain. The key difference between what I might call the traditional means of customs risk management and current or planned approaches is the necessity for much tighter integration between customs administrations and the private sector. By 'tighter integration' I mean the involvement of industry at a much earlier point in the risk management cycle, indeed at the risk identification stage and then subsequently through the risk analysis, risk assessment and risk treatment stages.

It is important for customs administrations to understand the supply chain and to take effects on the supply chain into account when designing and implementing policies on supply chain security. In this regard it must be acknowledged that industry has the best insight into its own supply chain, both upstream and downstream and has a vested interest in removing as much cost as possible out of that supply chain. Industry has no wish to have its goods sitting on a wharf while a customs official decides what risk it represents and is going to be supportive of any policy or program that encourages transparency and predictability within the supply chain. For that reason globally accepted standards on supply chain security and AEO programs that achieve mutual recognition between trading partners should be strongly supported as improving transparency and predictability. They are in fact an important risk treatment for most

⁹ Quoted in "Customs Rattles the Supply Chain", March 1, 2006 edition of CIO Magazine

supply chain security risks as are some emerging technologies such as RFID and smart containers.

It is well reflected in Customs strategies that ask companies to assume responsibility for their supply chain security no matter who has physical custody of the goods at a particular point in time. An example of such a strategy is the US C-TPAT Program where as consideration for assuming that responsibility the government offers the benefits of reduced intervention in relation to the cargo and faster clearance¹⁰. It is also reflected in the EU concept of "Authorised Economic Operator". It should be noted however, that the benefit quid pro quo is important and a current weakness in many nascent programs is that such benefits are often either not well articulated or illusory.

Programs like C-TPAT and the Australian AEO pilot are recognition that the interdependence that always existed up, down and across the international supply chain also includes a reliance on government agencies such as Customs that regulate that supply chain. It was axiomatic that a failure of one link in the supply chain can put the whole supply chain at risk but it is interesting that there is now an increasing appreciation that government is also a link in that supply chain and can have an equally positive or negative impact on its performance. For that reason, multinational firms in particular are including improved relationships with customs administrations in their supply chain management strategies.

Managing supply chains involves the management of three fundamental flows: materials, information and funds. Public infrastructure plays an integral role in supply chains for the unimpeded movement of each of these flows.¹¹ A key component of that public infrastructure is Customs and the systems and business processes it adopts to manage the information it receives from industry for clearance of cargo.

A key Customs strategy is to collect as much information as it can about cargo about to enter their jurisdiction and at as earliest a point in time as possible to allow adequate profiling and subsequent data mining to identify and analyse anomalies in that data. This was one of the principal justifications behind the US Automated Commercial Environment (ACE) which is still being developed and Australia's Integrated Cargo System (ICS), although serious questions remain as to whether it has been achieved.

The required information can be captured in paper form or electronically. In the vast majority of cases (certainly within customs administrations of developed economies), information is captured electronically. When it is so captured, it will usually be communicated over several computer and telecommunications systems, much of which won't be proprietary to the companies providing the information, and much of which will be regulated by government agencies. This therefore also represents vulnerability for

¹⁰ For example, the toymaker Hasbro spent just under \$200,000 on its up-front C-TPAT compliance and spends an additional \$112,500 a year maintaining it. Since it became C-TPAT certified in November 2002, its inspections have dropped from 7.6% of containers coming into the US in 2001 to 0.66% in 2003. In 2003 the company imported about 8,000 containers, and port authorities charge around \$1,000 per inspection. Hasbro is therefore saving about \$550,000 per year in inspection costs alone – Quoted at www.cio.com/archive/030106/supply_security.html

¹¹ MIT Center for Transportation and Logistics, "Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains" August 8, 2003

supply chains and should be as transparent as possible to minimize the risk of information leakage.

At a more micro level the 'information collection' strategy has been and remains somewhat controversial, particularly as regards the most recent data proposal by the United States, referred to colloquially as "10 + 2". It goes beyond the WCO's approach to standardising customs data elements and would make companies collect information that they haven't collected before at an earlier point in time than they are used to. For example, few companies would know where on a ship its container is located, but the new data rules would require that information.

To provide a further example, US CBP are piloting an ACE addition called the Advance Trade Data Initiative (ATDI), which requires importers to share with Customs every bit of information about a shipment, including the purchase order, which port it passes through, proof of delivery and its final destination within the United States. There are fears that CBP plan to make ATDI participation a requirement for companies to achieve tier-three C-TPAT certification. I don't think I need to highlight the cost and privacy implications for international trade of that type of initiative, even if it does "...reduce the size of the haystack" as US Senator Patty Murray of Washington puts it.

Information is critical and it is what lubricates supply chains. It is equally important to Customs risk identification process. How and what information is made available for regulatory purposes is key. There are particular challenges for customs administrations and companies engaged in international trade where information management is concerned because the reality is that for certain manufacturing operations and freight forwarders in particular countries, they cannot send EDI messages and there is much less visibility in that part of the supply chain. This problem is exacerbated in supply chains that utilize multiple sourcing.

Policy and standards set by customs administrations must be able to recognize this and companies must be prepared to invest in improving information flows to provide that visibility. As far as possible customs administrations should be leveraging commercial information flows for their data input, not imposing additional obligations that aren't reflected in commercial data holdings. There is a wealth of information in standard supply chain documentation such as purchase orders that can be utilized for securing the supply chain.

Can I conclude by stating that the greatest benefits for both customs administrations and industry rely on compatibility between initiatives and mutual recognition. Of course, governments need to be able to say that they have improved security without sacrificing the efficient movement of goods across borders and company CEOs must be able to say that their companies are competitively better off because of their investments in supply chain security. Neither objective is mutually exclusive nor are they inconsistent and closer integration between government and the private sector on supply chain security creates the environment where such statements can be positively made.