International Transport Forum

TRANSPORT FOR A GLOBAL ECONOMY

Challenges and Opportunities in the Downturn

FORUM 2009 • 26-29 May • Leipzig

WORKSHOP 4

Ensuring a Secure Global Transport System

Maritime Transport Security Regulation: Policies, Probabilities and Practicalities

David Widdowson and Stephen Holloway
University of Canberra, Australia

OECD

MARITIME TRANSPORT SECURITY REGULATION: POLICIES, PROBABILITIES AND PRACTICALITIES

David WIDDOWSON and Stephen HOLLOWAY

Centre for Customs and Excise Studies
University of Canberra, Australia

Abstract

This paper examines the global regulatory environment that has emerged as a direct result of the events of September 2001, with particular reference to maritime shipping and container transport security. In examining the range of regulatory initiatives that have been introduced by national, regional and international policy makers, it analyses the appropriateness of the various policy responses from the perspective of risk management and commercial practicality. In doing so, the authors identify key features of an effective regulatory compliance regime, and the likely impact of specific policies on both regulatory control and trade facilitation.

The paper concludes that many government responses to the international security threat merely lead to an increase in the regulatory burden on honest traders, and achieve little in the way of enhancing their ability to identify potentially high risk consignments. It also identifies the need for a balanced and cost effective approach to regulation in which the elements of both enforcement and incentives to comply with regulatory requirements are present, in preference to a prescriptive approach that is likely to be not only less cost-effective but also more disruptive to commercial operations.

Context

The regulatory focus on the international supply chain changed dramatically on September 11, 2001 from one that was generally facilitative to one that placed the security of the supply chain at the centre of border management policy.

Border control, of which supply chain security is an element, has always formed part of the regulatory continuum, and since the late ’80s there has been a global effort on the part of regulators to achieve an appropriate balance between facilitation and regulatory control. However, there is clear evidence to suggest that following 9/11 the balance has been heavily tilted towards regulatory intervention (Widdowson 2006).

More significantly, whereas border control issues have traditionally centred on commercial illegality (for example, duty evasion) or smuggling of prohibited goods (for example, narcotics), the events of 9/11 highlighted the potential for the supply chain itself to be utilised by terrorists to cause physical and economic damage, and a proliferation of security-focused control regimes followed.

Indeed, supply chain security promptly became the priority issue, and with the three-day closure of United States (US) borders, the economic impact of any breakdown in the supply chain became obvious to everyone involved in international trade. A number of initiatives, ostensibly introduced to improve the security of the supply chain, were developed: firstly, by the United States and subsequently, by other countries and international organisations. The US initiatives have tended to lead the supply chain security agenda and that continues to be the case, although with increasing controversy and considerable resistance from other countries and the private sector. The highly criticised '10+2 Rule' and the 100 per cent container scanning initiative are cases in point.

Such rigorous opposition raises the question of whether the current nature and extent of supply chain regulation are appropriate and whether the supply chain is becoming over-regulated to the detriment of the efficiency and effectiveness of both government and business. This paper analyses the appropriateness of the diverse regulatory regimes from the perspective of risk management and commercial practicality.

Elements of effective regulation

Regulatory compliance management

Models for managing regulatory compliance are generally considered to fall into two broad categories: normative and rationalist (INECE 2009). The normative model advocates the encouragement of voluntary compliance through cooperation, support and the positive reinforcement of compliant behaviour. The rationalist model, on the other hand, advocates an enforcement approach, the focus of which is the deterrence of non-compliant behaviour by punitive means.

In practice, regulatory agencies will generally adopt compliance management strategies that incorporate both normative and rationalist elements. These elements effectively represent opposite ends of a compliance management continuum that seeks, firstly, to encourage voluntary compliance but which includes a range of punitive measures that may be applied in the event of non-compliance. In such circumstances, the severity of the measures applied should appropriately reflect the level of non-compliance, in other words 'let the punishment fit the crime'.

A number of issues need to be considered when determining the best 'mix' of elements that should be present in a regulatory framework. These include the need to achieve a cost-effective outcome consistent with the desired policy outcome; the nature of the operational environment that is being regulated including the commercial practices that apply; and the extent to which the regulatory requirements are likely to impact on the operational effectiveness of the activity being regulated.

Consequently, most compliance management regimes will comprise a combination of regulatory approaches, with the specific components of a particular scheme being dependent on the scope of the risk that is to be treated and the demographics of the regulated population. Parker describes this approach as 'compliance-oriented regulation', in which the elements of both enforcement and incentives are present:

> *It is a holistic approach toward regulation in which mixes of regulatory strategies appeal to the complexity and variety of motivations underlying compliance. The emphasis is on the substantive policy objectives of the regulation and whether the regulatory policy instruments chosen are capable of accomplishing those objectives,*

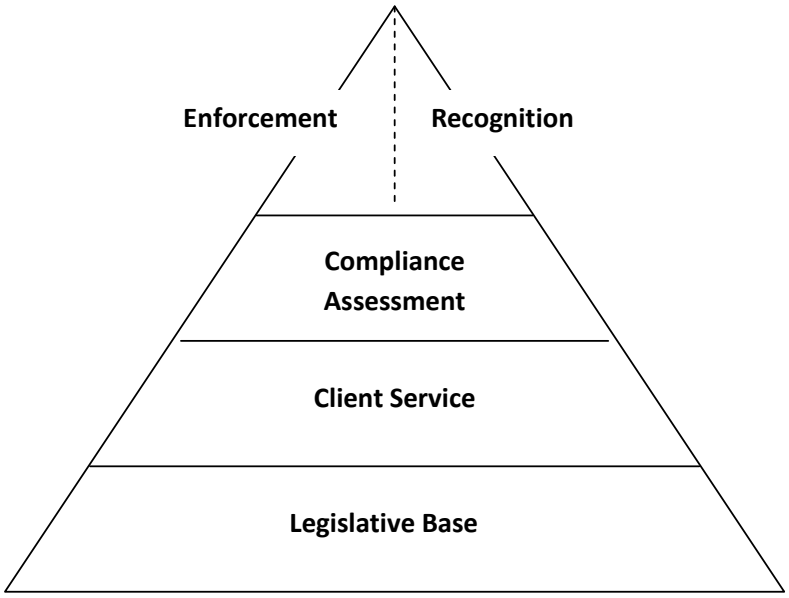
not on compliance with rules that may or may not be effective at achieving the desired result (Parker 2000, p.534).

Legislative base

Nevertheless, rules are at the core of any regulatory regime, and the role of the regulator is to ensure compliance with those rules. The point that Parker makes is that there needs to be a clear understanding of what the policy makers are trying to achieve, and that when developing an associated regulatory regime, the achievement of the policy objective must remain in focus. Compliance with poorly constructed rules will do little to achieve such policy objectives. It is therefore incumbent upon regulators to continually question the validity of the rules that have been established in order to ensure their ongoing relevance to the policy aim. In the post 9/11 political climate, however, it takes a very brave person to question the validity of rules that have ostensibly been designed to mitigate international transport security risks. This issue will be addressed later.

Several models have been developed to identify better practice in regulatory compliance management, all of which emphasise the need for an effective legislative base. A simplified model[1] is shown in Figure 1. An appropriate legislative framework is an essential element of any regulatory regime since the primary role of the regulator is to ensure compliance with the law. Regardless of the compliance management approach that it is supporting, the legislative framework must provide the necessary basis in law for the achievement of the range of administrative and risk management strategies which the administration chooses to adopt.

Figure 1. **Simplified Compliance Management Pyramid**



Source: based on Widdowson (2004)

Informing the regulated community

An appropriate range of client service strategies, including effective consultation arrangements and clear administrative guidelines, is necessary to provide the commercial sector with the means to achieve certainty and clarity in assessing their liabilities and entitlements. In 1997, when calling for an urgent international process of regulatory reform, the Organisation for Economic Co-operation and Development (OECD) stated that such reform should include more flexible approaches to regulatory compliance management, with the longer-term goal of shifting governments 'from a culture of control to a culture of client service' (OECD 1997).

Such a cultural shift required regulatory authorities to accept the view that strategies other than control strategies represent legitimate means of mitigating the risk of non-compliance, and are critical to achieving an effective balance between facilitation and regulatory intervention. Indeed, it is of critical importance to ensure that the commercial sector is provided with the ability to comply with regulatory requirements. They need to know the rules. If they do not know, how then can they be expected to comply? While ignorance of the law may be no excuse, it explains many instances of non-compliance and, consequently, the need to provide meaningful advice to those who are being regulated is essential.

Compliance assessment

At the third tier of the pyramid (Figure 1), the elements of compliance assessment come into play which in the maritime transport context, generally include data screening, documentary checks, risk-based scanning and physical examinations as well as pre- and post-shipment audits and investigations. Effective compliance assessment must include strategies that are designed to identify both compliance and non-compliance, which addresses one of Parker's key concerns, that is, that regulatory authorities tend to focus solely on the detection of non-compliance. The reason for the traditional focus on non-compliance stems from the fact that, for most regulators, the only recognised 'result' of compliance assessment activities has been the identification of non-compliance, together with the associated enforcement action such as prosecution and/or monetary sanctions (Widdowson 2006). The saying, 'if it isn't counted, it won't get done' applies aptly to this situation. In other words, if management focus is solely on the identification of non-compliers, the identification of compliant traders will not be considered to be important by their staff.

In recent times, there has been an increased emphasis on a 'partnership' approach to assessing and achieving regulatory compliance, and a number of approaches that have been introduced in the transport security environment are discussed later. The government/industry partnership concept is based on the premise that companies with a good record of compliance require less regulatory scrutiny than those with a history of poor compliance, or those about which little is known. The partnership approach to security has also been adopted in other transport sectors such as the air transport industry's Known Shipper Program,[2] and its potential application to air passengers is also a topic for debate (Poole 2008).

A key element of the strategy seeks to provide highly compliant companies with certain benefits such as facilitated clearance arrangements, an entitlement to self-assess, and reduced regulatory scrutiny, which provide compliant companies with the incentive to demonstrate their commitment to comply with regulatory requirements.

The effectiveness of such arrangements hinges on a healthy working relationship between government and industry, based on partnership and trust, that is, a relationship which reflects a

mutual commitment to accountability and improving compliance. Such partnerships must be a two-way proposition with clearly identified costs, and benefits and responsibilities for both parties. Consistent with the cooperative, consultative approach which a partnership program is intended to achieve, industry should be invited to play a major role in identifying the range of incentives which may be made available under such an arrangement.

Provided such programs can achieve mutual benefit for both government and industry, the partnership approach is destined to succeed. However, if the anticipated benefits fail to materialise for either of the parties, the relationship is likely to be less than successful, particularly when would-be participants have made a significant investment in the initiative. Given that one of the parties to such a partnership is a regulatory authority, it is hardly surprising to learn that the benefits which fail to materialise are generally to the detriment of industry (Widdowson 2005).

Enforcement and recognition

In the process of assessing the level of compliance among industry players, regulators encounter two situations: compliance and non-compliance. The non-compliance spectrum will range from innocent mistakes to blatant fraud. If the error nears the fraudulent end of the spectrum, some form of sanction will need to apply, including administrative penalties or, in the more severe cases, prosecution and licence revocation.

Before determining the need for or nature of a sanction, however, it is important for regulators to identify the true nature of the risk by establishing why the error has occurred. For example, the error may be the result of a control problem within the entity, due to flawed systems and procedures, or it may be the result of a deliberate act of non-compliance. The type of mitigation strategy that should apply in such situations will depend on the nature of the identified risk and unless the act is found to be intentional, it may be appropriate to address systemic problems within the entity, or to provide that entity (or perhaps an entire industry sector) with advice on particular compliance issues, or provide formal clarification of the law through binding rulings or other means (Widdowson 1998).

Measuring compliance

Determining the effectiveness of the regulatory approach to reducing non-compliance is one of the difficulties confronting regulators. At the centre of this challenge is the quality of information and the resources to monitor compliance. It may be difficult or even impossible to obtain accurate and timely data about compliance, and even more difficult to establish a trend with respect to that data particularly if there is no compliance baseline against which the data can be measured. For example, compliance may be improving but without a baseline, it will be difficult to identify that improvement and even more difficult to determine if it is the result of a specific regulatory approach or not, particularly if the nature of regulation is changing at the same time. The incorporation of relevant compliance indicators and an evaluation process into the regulatory scheme at the outset is therefore very important.

Regulation of Small and Medium-sized Enterprises (SME)

Another challenge for regulators is to avoid disadvantaging small and medium-sized enterprises (SMEs), which generally rate poorly in ‘compliance’ because they lack the capacity to comply, often due to a lack of resources or knowledge. An example from environmental regulation that illustrates this point is the United Kingdom (UK) SME Environment Survey

conducted in 2003 (NetRegs 2003). That survey noted that SMEs comprise more than 99 per cent of the 3.7 million businesses in the UK and generate about 60 per cent of its commercial waste and as much as 80 per cent of the pollution in England and Wales. Yet 82 per cent of the SMEs could not name, unprompted, any environmental legislation, and 77 per cent had not taken any measures aimed at reducing harm to the environment.

SMEs are significant participants in international trade but are not necessarily well catered for in the various supply chain security initiatives that have been implemented to date. In many countries, they constitute over 95 per cent of market participants and account for more than half of employment in the national economy as well as in the Gross Domestic Product (GDP). With respect to international trade, parties involved in the international movement of cargo are heavily represented by SMEs.

The World Customs Organization (WCO) recognised quite early in its development of the SAFE Framework that it should be implemented in a transparent and predictable way 'in order to provide a level playing field for both SMEs and large companies'. The WCO also noted that SMEs need 'adequate support, training and guidance to build their capacity for security requirements' and that they require 'tangible benefits in return for being certified as Authorised Economic Operators (AEO) by meeting a set of minimum security standards in the Framework' (WCO 2004).

Management-based regulation

Some of the issues confronted by regulators when designing a cost-effective regulatory scheme, including the importance of acknowledging compliance diversity within the regulated population, have already been identified in this paper. A sub-set of compliance-orientated regulation that seeks to address these issues and the challenges associated with risk management is known as 'management-based regulation'. This approach provides greater flexibility to business in meeting regulatory and risk management objectives and is focused on outcomes, the importance of which has been discussed previously.

Management-based regulation is a concept that leverages business knowledge and experience to achieve the regulatory objective: 'firms are not mandated to adopt specific risk protection technologies or practices, nor even necessarily to achieve specific limits on levels of risk or other measures of performance. Rather, firms are mandated to study their operations comprehensively and develop their own management strategies suited to the risks they identify in their operations' (OECD 2008).

Because management-based regulation leverages existing business processes, it has the potential to be much more cost-effective than prescriptive regulation and is certainly less disruptive of those business processes. It is also more likely to encourage innovation in managing compliance risk since businesses are more likely to comply with their own internal rules and procedures than with those imposed externally by government. Indeed, there is empirical evidence that suggests that management-based regulation can lead businesses to make risk-related behavioural changes (Bennear 2007).

Using this approach, regulated entities are often expected to develop plans or management systems that comply with criteria prescribed by the regulatory authority, for example, security plans under the International Ship and Port Security (ISPS) Code, or physical security and access restrictions under the various customs AEO and related programs. The regulatory approach may include a requirement for certification by government regulators or third-party

auditors of the plans and management practices, together with evidence of compliance (OECD 2008). The OECD has recognised the importance of compliance measurement with this regulatory approach as for compliance-orientated regulation generally:

> *Performance standards focus attention on desired outcomes and provide flexibility to find less costly or better solutions but making them work depends on being able to measure and monitor performance. Sometimes it is difficult to operationalise the desired outcome into an enforceable regulatory standard, or sometimes it is prohibitively costly for the regulator to monitor outcomes… (OECD 2008, p.10).*

This is an important issue with respect to regulation of the international supply chain because it is particularly difficult to monitor or measure supply chain security risk in a way that is meaningful to business in terms of keeping that risk below a specified level. There is no such thing as 'zero risk' in the international supply chain and, at least at an operational level, businesses are often better positioned to identify risk in their supply chain than regulators, although that changes as the focus moves to broader strategic risk.

This then leads to a discussion of risk management in the context of the maritime security environment and in particular, whether that risk can be identified in a way that facilitates the design of cost-effective and efficient regulatory approaches to supply chain security that meet government and private sector concerns.

The nature of maritime transport security risk

International trade and logistics in the 21st century

The changed nature of maritime transport security risk reflects the increase in the volume and complexity of international trade itself. Technological innovation leading to the twin benefits of vast improvements in the speed of transportation and communications and the lowering of costs, has resulted in better access to overseas markets and a much greater diversity among entities involved in international trade. It has also resulted in exponential growth in the use of containerisation in maritime transport.

In 2006 the United Nations Conference on Trade and Development (UNCTAD) highlighted the fact that trade represents merely a part of a global supply chain. It estimated that about one-third of international trade in goods involves trade in unfinished goods and components, and a similar percentage represents trade within the same company (UNCTAD 2006). It is likely that these percentages have increased since the time the UNCTAD report was prepared and indeed, the WCO estimates that the percentage of intra-company trade is now closer to 50 per cent (WCO 2008).

The majority of such trade is moved (in a documentary sense) within an integrated global logistics system in diminishing timeframes to meet global sourcing and just-in-time business models that emphasise low inventory. Companies manage a continuous flow of goods that are transported as part of an intricate logistics and supply chain management system that ensures delivery at precisely the moment they are required for use as an input in production. The benefits in cost savings and efficiency are significant, but so are the risks when considering that even a short disruption to that supply chain can have considerable financial consequences (Swedish National Board of Trade 2008).

A case study that serves to illustrate the current complexity of international trade examines a single component for Apple's iPod Nano – its central microchip. That microchip is provided by a

US company (PortalPlayer). The core technology of the chip is licensed from a British company (ARM) and is modified by PortalPlayer's programmers in California, Washington State, and Hyderabad. PortalPlayer works with microchip design companies in California which provide the finished design to a company in Taiwan that produces 'wafers' imprinted with hundreds of thousands of chips. These wafers are then cut up into individual disks and sent to another facility in Taiwan where they are individually tested. The chips are then encased in plastic and readied for assembly by Silicon-Ware in Taiwan and Amkor in the Republic of Korea. The finished microchip is then warehoused in Hong Kong before being transported to mainland China where the iPod is assembled.[3]

The iPod example of global sourcing is becoming an increasingly common feature of modern supply chains. It highlights not only the potential risks but also the difficulties of managing those risks from either a business perspective in ensuring just-in-time delivery of components, or from a business and government perspective with respect to securing the supply chain from both a commercial and regulatory perspective, including potential security threats. The reality is that there is a convergence of interest between business and government in maintaining a secure supply chain. It requires cooperation and coordination to function effectively and to minimise the risks of disruptions in the flow of goods. This collective benefit in supply chain security is recognised in the study undertaken by the Swedish National Board of Trade (2008).

The development and implementation of strategies to mitigate maritime transport security risks is complicated by the high degree of interdependence and associated network characteristics exhibited by modern global supply chains. This has created great uncertainty as to where the risks actually begin and end, since what at first may look like a minor event can quickly turn into a full-blown crisis (OECD 2009b). An often quoted example is the fire at a single-source supplier used by Ericsson which resulted in US$400 million in lost sales for Ericsson, a drop in stock price of 11 per cent and the eventual exit of that business line. The principle is illustrated on a global scale when one considers that the current financial crisis resulted from regulatory approaches that were adopted with relative confidence but which failed to identify the potential global ramifications of a seemingly isolated risk in one sector of an economy.

To this point, the discussion has been mainly about generic risks that flow from the complex and interdependent nature of modern supply chains, but the post-9/11 focus on counter-terrorism has required the international community to seriously consider the ephemeral characteristics of terrorist risk. Unlike other risks such as accident risk where the events are unintentional and their likelihood can be reasonably estimated from empirical observations, the probabilities associated with a terrorist attack are much harder to quantify (OECD 2009a). The OECD suggests two reasons for this:

> *First, terrorist attacks are relatively infrequent. This is especially true of attacks that belong to the class of extreme events, with low probabilities, major consequences, and possibly spillovers into connected systems. For such infrequent events, past events carry little information on future probabilities.*
>
> *Second, attaching probabilities to intentional acts is particularly problematic because of the possibility of strategic behaviour: terrorists adapt their strategy to changes in the security environment in which they operate. Since little is known about how they will respond (because the set of available strategies is very large), it is not clear how security policies or other relevant changes affect probabilities. In sum, terrorist attacks are not characterised by risk but by uncertainty, meaning that no credible objective probability can be assigned to their occurrence (OECD 2009a, p.6).*

What can be said with some degree of certainty is that the nature of risk in the maritime transport environment requires flexibility and resilience to be engineered into regulatory initiatives to ensure their effectiveness, and that this notion of flexibility and resilience requires cooperation between and across business and government rather than a parallel and self-centred or 'silo' approach. It also requires both national and international perspectives that acknowledge the increased connections and interdependencies between and among economies. As the OECD points out in its studies of country risk management, when discussing the necessity for collaboration between government agencies, there may be an exposure 'to unforeseen vulnerabilities when risks arise that do not fit neatly within the remit of one particular department...Indeed efficient risk management may be compromised by the inability to deal effectively with bottlenecks in the exchange and analysis of information or to set priorities informed by the entirety of a country's risk portfolio' (OECD 2009b). Furthermore the risk management efforts of one company can be nullified by the inattention or inadequacy of a single supply chain partner (Closs *et al*. 2008).

If it is accepted that containerised cargo is one of the unique features of modern international cargo transportation and that there is some potential for it to be utilised by terrorists or by organised crime, then one of the critical supply chain security risks to be analysed relates to the international movement of containers and more specifically, to what is inside those containers.

> *The specific stuffing location is paramount from a security perspective because it represents the last point in the container transport chain where the physical contents of the container can be visually identified and reconciled with the commercial invoice and/or bill of lading. After the doors are shut and sealed and until they are re-opened by Customs or by the consignee at the final destination, all information regarding the contents of the container (e.g. such as the manifest, the bill of lading and even the commercial invoice) are necessarily unverified. Thus the originating shipper has a critical role to play in the container security by generating a clear, accurate and complete inventory of the physical contents of the container. Proper site security, stuffing procedures and oversight of the stuffing process are necessary for this important link in the chain to be secure (OECD 2005, p.29).*

It is axiomatic that cargo containers are at their most vulnerable in terms of having unlawful cargo introduced into the supply chain when they are at rest and least vulnerable when they are in motion (OECD 2005). This has driven a great deal of the regulatory design thinking around supply chain security measures and placed particular emphasis on those nodes in the network where the container is handled and/or stored.

The OECD makes another important point when it notes that most international container trade passes through one or several ports. The US Container Security Initiative (CSI) focuses its security measures on those ports with the largest export volumes to the US. However, it should be noted that there is a much larger number of 'feeder' ports that are still involved, albeit in a minor way, and that the ports that tranship cargo through the major hubs represent a potential risk node in the broader supply chain dynamic. It is true that it is incumbent on these ports to put in place security measures in accordance with the requirements of the ISPS code, but the effectiveness of those measures is in turn dependent on the commitment to supply chain security of the governments that are responsible for them and the quality of the relevant regulatory framework and its enforcement.

A common thread that can be discerned from the various risk characteristics of the modern supply chain is the importance of supply chain *visibility*. Visibility represents the key to early risk

identification and response and is a precondition for supply chain resiliency. It must therefore be considered to be of equal significance to both government and business.

At present most supply chain security initiatives have as their foundation a concept of 'layered security'. This concept attempts to design redundancy into the system so that security breaches at one level can be guarded against at a subsequent level. Such initiatives acknowledge that an insecure supply chain has adverse effects on both business and government, and that all to a greater or lesser degree require public and private sector participation to be embodied in the proposed regulatory measures. However, it is suggested that a number of these initiatives are less efficient and effective in their design than others because they fail to contribute to supply chain visibility.

Supply chain visibility: a business perspective

The Global Supply Chain Benchmark Report published by the Aberdeen Group in June 2006 emphasises the importance of supply chain visibility to business. It found that a lack of supply chain visibility coupled with poor automation impacts a company's bottom line through longer lead times, larger inventory buffers, budget overruns, and demand-supply imbalances. In particular, large multinationals are of a scale where poor visibility and uncoordinated multi-tier processes result in significant 'just-in-case' inventory carrying costs, premium freight expenses, and extended cycle times (Aberdeen Group 2006). Some particularly relevant findings from the Report include:

- Some 79 per cent of companies said that the lack of supply chain process visibility is their top concern.
- 82 per cent of companies are concerned about supply chain resiliency, but just 11 per cent are actively managing this risk.
- The top five 'gap' areas relating to supply chain risk were risk profile of vendors (56%), supply chain security (51%), logistics capacity and congestion (47%), risk profile of country (46%) and weather disruptions and natural disasters (44%).
- In addition, 47 per cent wanted to improve the data quality of the event messages, including timeliness, completeness, and accuracy of those messages.
- 91 per cent of companies reported that unexpected supply chain costs were eroding their anticipated low-cost country sourcing savings, with transportation budget overruns being the top culprit.

The Aberdeen Group's report reveals that improvements in supply chain risk management are being achieved through the adoption of two core strategies. Firstly, through 'increasing logistics and supply agility by ensuring alternate suppliers, carriers, routes, and the like are arranged' and secondly, by 'improving visibility and automation of supply chain activity' both upstream and downstream in the supply chain.

Bearing in mind the importance of compliance (performance) measurement, multinational businesses are increasingly measuring the performance of their supply chains via the concept of 'total landed cost'. The Aberdeen Group's research shows that the best performers are those companies that have been most successful in reducing their total landed costs and documentation. These companies are 'twice as likely to have current budgeted trade compliance

projects as their peers'. It is further noted that 'as regulatory oversight intensifies, enterprises are finding increased value in moving to a single trade compliance platform for the entire company that enables consistency of product classifications and restricted party screenings and provides a common view of compliance activity and trade costs' (Aberdeen Group 2006).

In this context it can be argued that supply chain visibility and resiliency are critical characteristics of an international compliance strategy, and that a focus on trade compliance is as important to business as it is to regulators. Both are seeking to maintain security across the supply chain, although motivated perhaps by different objectives. As the Aberdeen Group's report (2006) states:

> *Managing international logistics is not like managing an extended domestic supply chain; it's fundamentally a multi-party process fraught with greater unpredictability in quality, lead times, costs, and risks. Rather than create the absolute-lowest-cost fixed network, leaders are building into their logistics networks more points of flexibility. This helps them continually scan their environment for bottleneck symptoms or spikes in demand and take action.*

Supply chain visibility: a government perspective

Supply chain visibility is equally as important for governments because greater supply chain visibility provides regulatory authorities with the information they need to analyse risks, identify high risk or suspect shipments and target potential security threats. The critical aspect here is 'information', since the regulator's ability to identify and treat risk is dependent on the timeliness and quality of information. If the information that is provided to commercial operators and regulators is inaccurate or intentionally false, the best regulatory scheme in the world will be unable to achieve its objectives in the absence of other sources of intelligence. This theme is further explored later in this paper.

Supply chain visibility in 'real-time' allows a rapid response to emerging risks and if this is combined with effective risk management systems that include proactive event and exception management,[4] the whole process of supply chain security is significantly enhanced. End-to-end supply chain visibility, although difficult to achieve, improves responsiveness for business (production rates and shipment lead times) and government (early risk identification).

The international movement of cargo is far from being fully visible because there is no single regulatory agency with end-to-end supply chain responsibility. As the OECD has previously observed, the most vulnerable period for the container is at the time of stuffing, before the shipper seals it. The system relies on the trusted shipper, and the majority of stock is presumed to be safe. However, the bill of lading represents a weak point in the chain: how do the authorities or downstream industry players know what is actually packed in the container? The bill of lading is rarely verified through inspection of the containers after packing or during transport; and road transport, where the container is in the hands of a single person for a lengthy period of time over large distances, is especially problematic (OECD 2005).

The ideal visibility outcome would be *visibility on demand* for government and business. This could only be achieved through close integration of relevant government and business logistics systems. This concept has been discussed at length in the customs environment as best practice with respect to achieving seamlessness in cross-border transactions and is predicated on government having direct and secure access to commercial data for risk assessment purposes. Although some may claim that this ideal has been achieved in the context of 'single window'

initiatives, the contrary is argued here. A true single window with on-demand access to existing commercial data by government and other stakeholders such as port authorities, freight forwarders and the like has yet to become a reality. While some of the more progressive port community systems may be presented as role models in the port environment,[5] a similar solution in the broader supply chain is far from being a reality.

Indeed, there may be a degree of resistance among participants in international trade to share with government what in most cases represents valuable commercial information for fear of competitors gaining access to price-sensitive and competitive information. As Dahlman *et al*. (2005) state:

> *Large shipping companies have information on the containers they transport and where they are at any given time. Smaller feeder companies are usually less organized. The information systems are unique to each company and do not interact with those of harbours or customs authorities. This information is of commercial value, and it is unclear how much information shipping companies are willing to share, and with whom and under what conditions.*

While there is no argument that a lack of timely and accurate data reduces supply chain visibility, the major barrier to end-to-end supply chain visibility remains this lack of integration and its surrounding challenges, including the technology and infrastructure limitations of the various stakeholders up and down the supply chain, which in many cases includes government.

The OECD recognises such shortcomings in its identification of common challenges to effective risk management, which include 'misinterpretation or misrepresentation of data, communication bottlenecks and logistics breakdowns, which may increase with every step taken between a source of information and its use by decision makers. Overarching, all-hazards policy frameworks promote coordination of highly specific expertise, development of information-sharing arrangements, improvement of data integration capacity, investment in training civil servants and cooperation exercises across multiple agencies involved in country management (OECD 2009).

The evolution of current supply chain security initiatives

SITPRO has developed a useful categorisation for the various types of international trade security measures that have been introduced recently:

- *Umbrella,* aimed at security risks in their broadest sense
- *Goods specific,* aimed at risks specific to individual types of goods
- *Control specific,* aimed at meeting narrowly specified control objectives
- *Safety,* concerning the safety of staff and use of critical infrastructure
- *Commercial,* business-based initiatives to manage transport and supply chain risk (SITPRO 2008).

In this paper, the SITPRO categorisation has been adopted when describing how the various supply chain security initiatives that have been implemented, or are about to be implemented, have evolved since the events of 9/11.

Many of the initial supply chain security measures may be described as umbrella approaches, that is, they are designed to deal with security risk in the supply chain at the broadest level. The first of these initiatives was the US Customs-Trade Partnership Against Terrorism (C-TPAT) program.

In essence, C-TPAT is a voluntary government-business program that encourages cooperation between US Customs and Border Protection (CBP) and the international trading community in an effort to increase the level of international supply chain security. The intention is that, in exchange for businesses meeting CBP-designed security standards and becoming C-TPAT certified, participants in the program should receive certain benefits such as reduced inspections and priority processing. Manufacturers, importers, carriers and service providers participate by submitting detailed self-appraisals of their supply chain security practices, and these are periodically verified by CBP. However, according to Laden (2007, p.78),

> *...the validation process is clearly the Achilles heel of the C-TPAT program. Most SCSS validators have only enough knowledge and experience to complete a very cursory review of security protocols at a certain facility. In fact, the validation program has earned a reputation of being more of a 'feel good exercise' than a true validation and test of a company's supply chain security program. Many validations take two hours or less, and are generally held in one of the more desirable travel destinations, rather than where the risk actually lies.*

This focus on relatively broad supply chain security risks and the development of an overall framework for managing supply chain security has been subsequently reinforced with the introduction of the International Maritime Organization (IMO) International Ship and Port Security (ISPS) Code, the World Customs Organization (WCO) SAFE Framework of Standards, the US SAFE Port Act, the International Organization for Standardization (ISO) supply chain security standard (ISO 28000), and the various Authorised Economic Operator (AEO) programs such as those implemented by Japan, Singapore and the EU, which have largely been modelled on the WCO SAFE Framework.

Other security initiatives are, however, much narrower in focus. Such initiatives are not only more specific, but have been driven 'top-down' by government, and have involved far less collaboration with the private sector. A *goods specific* example is the US Bioterrorism Act[6] which is designed to assist the US Food and Drug Administration (FDA) to determine the source and potential cause of any contamination of imported food and beverages. The Act facilitates such identification by requiring registered food facilities[7] to provide the FDA with consignment information prior to importation into the US. Depending on the mode of transportation, parties involved in importing these products are required to provide the information two to eight hours prior to arrival.

Another early initiative was the US Container Security Initiative (CSI). Introduced in 2002, CSI is an example of a *control specific* initiative, the focus of which is predominantly procedural compliance rather than on implementing a regulatory framework that is aligned with contemporary supply chain management practices. CSI involves bilateral arrangements between CBP and other customs authorities that are designed to identify high-risk cargo containers before they are loaded on vessels destined for the US.

Under the CSI initiative, economies agree to the posting of US officials at ports which ship large volumes of goods to the US, and for them to examine high-risk maritime containerised cargo (generally through X-ray and radiation scanning) before being loaded on board vessels

destined for the US. As such, CSI is an initiative that seeks to push US port security upstream in the supply chain to the port of origin of the cargo. At the time of writing, 58 ports, accounting for 85 per cent of container traffic bound for the US, were participating in CSI.[8]

Sarathy (2005) comments on a number of shortcomings in the CSI operation due to its reliance on receiving 'complete and accurate manifest data to analyse in deciding which containers to target for further inspection':

> *In Rotterdam the CSI team found that manifest data was not complete. The data was limited to containers actually transferred from one vessel to another in Rotterdam. Manifest data did not extend to containers that remained on board a vessel bound for the US which stopped in Rotterdam. Further, the CSI did not have manifest data on containers from Rotterdam which had arrived by truck, rail or barge from other countries (neighbouring EU countries as well as countries further afield in E. and Central Europe). Further, paper manifests were received at 40 different locations within the Rotterdam port. Dutch law sometimes prevented such paper manifests from being removed from their locations. These factors together made it difficult for CSI to receive accurate and complete and timely manifest data before the containers left Rotterdam.*

Sarathy observes that the information deficiencies demonstrated by the Rotterdam exercise led to the US Advance Manifest Rule (also referred to as the 24-hour Rule), which requires all ocean carriers or non vessel operating common carriers (NVOCC) to electronically transmit cargo manifests and entry data to the CBP Automated Manifest System 24 hours before the US-bound cargo is loaded onto a vessel at the port of export. In essence, the 24-hour Rule shifted responsibility for the provision of information from the foreign ports to carriers, forwarders and brokers, and in doing so, imposed additional maritime transportation costs. As noted by Grainger (2007), 'transaction costs amongst actors occur...where regulations and operational practices do not align'.

The 24-hour Rule is an example of a *control specific* initiative, the focus of which is predominantly on prescribed information and procedural compliance rather than on implementing a regulatory framework that is aligned with contemporary supply chain management practices. Other examples of *control specific* initiatives include the US 100 per cent container scanning initiative, the US Secure Freight Initiative and the US '10+2' Rule. Such initiatives are not solely being pursued by the US, however, as Sarathy (2005) notes:

> *...when the port of Le Havre joined CSI in Nov. 2002, the French Customs updated an existing form, and required shippers to file information on 36 data items twenty-four hours before goods arrived at the port. The data were incorporated in a 'Declaration de Surete (DS)' collected from shippers, exporters, brokers and freight forwarders; this report was actually more comprehensive than the US Customs' 24-Hour Rule document which required fifteen data elements...*

While it is true that maritime and other security initiatives are now ubiquitous, most responses to the threat of supply chain terrorism can be traced back to their US origins (such as the Le Havre initiative), and this continues to be the case. Two US programs that are currently being debated, and which the international community is watching particularly closely, are the 10+2 Rule and the 100 per cent scanning initiative.

The 10+2 Rule

Formally known as Importer Security Filing (ISF) and Additional Carrier Requirements, the 10+2 Rule is a US initiative that requires importers and ocean carriers to submit data elements to the US CBP in addition to the 24 or so data elements that they are currently required to provide.

According to Blegen (2009), 'This rather innocuously titled 57-page regulation contains what is likely to represent the single most significant change in the US import process in at least 15 years, and is the culmination of approximately two years of concentrated effort by CBP in the face of widespread trade opposition within the US'.

Section 203(b) of the US SAFE Port Act requires the Secretary of Homeland Security, acting through the Commissioner of Customs and Border Protection, to require the electronic transmission of additional data elements to improve high-risk targeting as advance information with respect to cargo destined for importation into the US prior to loading of such cargo on vessels at foreign ports. The additional data elements are:

1. Seller name and address (or number).
2. Buyer name and address (or number).
3. Importer of Record Number/Foreign trade zone applicant identification number.
4. Consignee number(s).
5. Manufacturer (or supplier) name and address (or number).
6. Ship to party name and address (or number).
7. Country of origin of the goods.
8. Six-digit Commodity Harmonized Tariff Schedule number.
9. Container stuffing location name and address (or number).
10. Consolidator name and address (or number).

These data elements are to be provided by the importer. The other two (2) data elements are vessel stow plan and container status messages which must be provided by the carrier.

It is widely considered that the rule goes beyond the legislation's intent by placing legal liability on the importer to obtain complete, accurate information from overseas sources, which may be impossible to obtain or verify before the cargo is due to be loaded on the US-bound vessel. Furthermore, shippers and forwarders are concerned about the associated IT programming costs, third-party filing fees and cargo delays while the importers locate origin and destination information that does not currently form part of the commercial data stream.[9]

The US Federal Office of Management and Budget has estimated that the 10+2 Rule could cost industry between US$350 million and US$600 million annually, and is closely examining the rule's economic impact to ensure that it does not place an undue burden on business in the current financial crisis and economic slowdown.[10] A recent article in the *Journal of Commerce* cites the US National Association of Manufacturers in relation to the possible impact of the Rule:

The association cites independent studies concluding that importers of manufactured goods incur a collective cost of $8.5 billion for each additional day added to the supply chain, partly related to additional inventory carrying costs. According to the NAM, a Purdue University and USAID study independently estimated that each day of shipping time saved is worth 0.8 per cent ad-valorem tariff for manufactured goods. Based on the value of total manufactured imports carried by sea vessels in 2007 ($1.04 trillion), a one-day delay would collectively increase the cost for US manufacturers by $8.5 billion annually. Manufacturers estimate at least a two-day delay, or $17 billion annually (Tirschwell 2009).

100 per cent container scanning

Another example of a *control specific* initiative is the US 100 per cent container scanning proposal. The US SAFE Port Act requires 100 per cent scanning of all US-bound container cargo by 2012 using non-intrusive inspection equipment, including imaging equipment which may use X-rays or gamma rays to create images of the containers' contents, and radiation detection equipment at foreign ports. A pilot program to test the feasibility of 100 per cent scanning has been conducted at six selected CSI ports.

This initiative attempts to push supply chain security further 'upstream', consistent with some of the other control initiatives highlighted earlier. However, while in theory the physical inspection of the contents of every container provides the best determination of a security risk, it is also one of the most costly and labour-intensive measures to implement. To illustrate the magnitude of the task, of more than 7 million containers that entered the US in 2002, approximately 10 per cent were inspected and scanned (up from 2 per cent prior to 9/11). In Rotterdam the figure is about 5 per cent and in the UK it is between 4 and 7 per cent (OECD 2005).

Many customs administrations undertake 100 per cent screening of containers in the sense that the associated information is screened, but none physically examine 100 per cent of their container traffic, either through the use of scanning equipment or otherwise. Indeed, this would be impossible with currently available technology and the volumes of containerised trade.

The proposal for 100 per cent scanning in the current maritime operating environment represents the antithesis of risk management. On the other hand, screening, which in many cases is now fully automated, forms an integral part of an appropriate risk management regime that assists in identifying those containers which may pose a security (or other) risk, and are therefore candidates for scanning and inspection. The 24-Hour Rule and similar requirements for advance information contributes to the screening process and the early identification of high-risk cargo.

The difficulties of achieving 100 per cent scanning coupled with physical inspection have been highlighted by a number of national and international organisations including the US General Accounting Office (GAO) and the OECD. The OECD comments:

The ability of machines even with the latest technology, is limited and identification of materials relies on the expertise of operators. X-ray machines assess the density of materials and sound an alert but the screeners need to judge and identify the materials by viewing the image and sometimes by physical search. The inspectors need to be well trained to interpret the x-ray images and other indicators produced by machines (2005, p.49).

Similarly, the GAO observes:

> *…international partners have expressed to DHS and Congress that 100 percent scanning runs counter to – and could adversely impact the implementation of – international customs security standards such as the SAFE Framework. Officials from the European Commission and CBP stated that unless additional resources are made available, 100 percent scanning could not be met...Given these resource issues, officials from CBP and European customs administrations stated that scanning all cargo bound for the US may actually provide a lower level of security. The officials explained that 100 percent scanning could result in diluting the current focus on high-risk containers. Under the current risk management system, customs officers are to base their reviews on the perceived risk posed by the cargo and, thus, are to review the scanned images of high-risk containers in a very thorough and detailed manner. However, according to CBP and WCO officials, if the scanned images of all containers must be reviewed, the reviews may not be as thorough because customs officers could lose focus due to the sheer volume of work. If images are not properly or thoroughly analysed, a degradation of security could result. Further, a European customs administration official reported that 100 percent scanning could have a negative impact on the flow of international commerce. The official also added that the 100 percent scanning requirement would disproportionately affect trade with developing countries (GAO 2008).*

The GAO has identified the following nine major difficulties with implementing the 100 per cent scanning mandate:

- Workforce planning.
- Host nation examination practices.
- Measuring the program's performance.
- Resource (cost) responsibilities.
- Logistics of space constraints at ports.
- Technology and infrastructure.
- Use and ownership of data when foreign seaports are involved.
- Consistency with risk management.
- Reciprocity and trade concerns.

As with the 10+2 Rule, there has been strident criticism from the private sector with respect to implementation of 100 per cent scanning and indeed from CBP itself. Such criticism covers a broad range of issues including, but not limited to, potential costs and delays,[11] staffing challenges,[12] the lack of physical 'choke points' where large numbers of containers can easily be scanned on their way through ports,[13] the complexity of the task required of those viewing the scanned images,[14] and the shortcomings of available technology.[15]

Appropriateness of the regulatory initiatives

Trade efficiency abhors regulatory complexity and uncertainty. Traders need transparency, clarity and predictability in order to transport their goods as quickly and efficiently as possible from origin to destination. The complexity that is reflected in a multitude of regulations applying to the same transaction, and the uncertainty resulting from differences in interpretation and administration add cost to an international trade transaction and can reduce the competitiveness of a particular export or investment destination. Consequently, there is a strong demand for standardisation, harmonisation and mutual (cross-border) recognition.

As previously noted, in the present political environment, any challenge to the validity of security initiatives can be quickly dismissed on the basis that it is seen not to be supportive of international anti-terrorism efforts. However, it is contended that the time has come to critically evaluate the appropriateness of supposed security initiatives, particularly in the context of contemporary risk management principles and commercial practicality. The latter is of particular importance given the internationally identified need to stimulate the global economy as a matter of priority. Indeed, the current economic climate is placing more emphasis than ever on minimising costs, and the nature and extent of supply chain regulation is understandably a key area of focus for traders. In this regard, no regulatory initiative that has the capacity to significantly impact the facilitation of international trade can be exempted from rigorous scrutiny.

Voluntary compliance programs

A significant number of the security-related regulatory initiatives that have been introduced in the maritime transport environment since September 2001 are representative of a management-based regulatory approach, and reflect many of the principles of compliance-orientated regulation, of which management-based regulation is a sub-set. These regulatory regimes also fall within SITPRO's category of 'umbrella' security initiatives, in that they are designed to address security risks in their broadest sense.

The WCO SAFE Framework, the US C-TPAT program and the various national programs that are based on the SAFE Framework's AEO concept are all considered to fall within this category. Importantly, all such programs are voluntary. Members of the international trading community are invited to join the various programs on the understanding that they will be able to derive benefits that are not available to those who choose not to apply for membership. In this regard, the various schemes do not impose any regulatory burden on the industry participants that they are not willing to accept, and the decision to do so is based solely on commercial considerations.

Each of the programs has a clear focus on supply chain visibility but in a way which encourages industry participants to address the required security risk outcomes in a relatively flexible manner. This is achieved by leveraging business knowledge, operating practices and information systems, with an opportunity for the regulators to verify industry's self-assessed findings. Also, by leveraging existing commercial practices and procedures in this way, any disruption to business processes is minimised.

The various programs also reflect sound principles of risk management by seeking to identify low-risk members of the trading and transport community. The principal aim of AEO programs is to provide customs authorities with a method of identifying those elements of the international supply chain that are secure, which allows them to focus their resources on potentially high-risk operators. Assessing the compliance levels of such companies, regardless of the result, provides

Customs with a clearer picture of compliance levels and the potential impact of non-compliance. This in turn greatly assists in determining where future compliance resources should be directed.

The notion of coordination and cooperation which are at the heart of modern regulatory compliance approaches discussed previously are well served by these voluntary compliance programs. Such programs help create a network of secure operations, they establish a base level of security standards, and help raise the overall level of security for global operations. Also, participation in voluntary programs helps to further build the partnerships between the public sector and private industry necessary to create a secure environment (Purtell & Rice 2007).

There are, however, a number of concerns with these schemes, all of which relate to the need to deliver the benefits that are being claimed by the authorities. Indeed, there is considerable doubt as to whether some of the identified benefits will ever see the light of day, particularly those associated with the mutual recognition of AEO status. According to the WCO:

> *The Resolution on the SAFE Framework...calls upon Customs administrations to work with each other to develop mechanisms for mutual recognition of AEO validations and authorizations, and Customs control results and other mechanisms that may be needed to eliminate or reduce redundant or duplicated validation and authorization efforts.*
>
> *Mutual recognition is a broad concept whereby an action or decision taken or an authorization that has been properly granted by one Customs administration is recognized and accepted by another Customs administration. The standardized approach to Authorized Economic Operator authorization provides a solid platform for long-term development of international systems of mutual recognition of AEO status at bilateral, sub-regional, regional and, in the future, global levels.*
>
> *In order for a system of mutual recognition to work it is essential that...There be an agreed set of common standards (WCO 2007, p.54).*

However, while some WCO members are interpreting the guidelines to require an AEO to demonstrate a high level of supply chain security (for example, Singapore), others are adopting a far broader interpretation which includes customs compliance generally. The EU, for example, requires an AEO to demonstrate:

- an appropriate record of compliance with customs requirements;
- a satisfactory system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls;
- where appropriate, proven financial solvency;
- where applicable, appropriate security and safety standards (European Commission 2007).

Clearly an unfortunate casualty of this failure to agree on basic AEO criteria is the concept of mutual recognition. If one administration requires an entity to demonstrate levels of both general compliance and security compliance before being granted AEO status, and another grants AEO status solely on the basis of security compliance, the achievement of mutual recognition is unlikely unless the parties are prepared to adopt a 'lowest common denominator' approach.

Another potential benefit that has attracted some attention is the potential for reduced insurance premiums, that is, the possibility that certification as an AEO or member of C-TPAT may result in a reduced risk profile and therefore lower premiums. However, the fact is that measures to improve security do not necessarily lead to a reduction in insurance premiums because insurance companies take a 'networked' view of the supply chain (as they should), and are therefore concerned that a 'secure' entity may be tainted by less secure entities that form part of their supply chain. This reflects the principle that any supply chain is only as good as its weakest link and risk attaches to the entirety of the supply chain, not just one entity within it (OECD 2009a). Indeed, it is not known if any participants in either an AEO program or the US C-TPAT program have received cheaper insurance by virtue of that participation.

Interagency cooperation

Coordination and cooperation are at the heart of modern regulatory compliance approaches, and the voluntary compliance programs described above provide an effective mechanism for public/private sector collaboration. Such programs are strengthened in terms of both their efficiency and effectiveness when they seek to incorporate a broader range of regulatory matters than those relating to a single authority. To achieve this, a significant degree of interagency cooperation is required.

The OECD has recognised the dangers of a one-dimensional or 'silo' approach by government that fails to acknowledge the connections and interdependencies of modern society. As it states in its discussion of Innovation in Country Risk Management:

> *...Over time highly defined areas of competence tend to develop in which numerous ministries, departments and regulatory agencies at various levels of government carry out operations in parallel and separate silos. A modern networked society with increased connections and interdependencies may be exposed to unforeseen vulnerabilities when risks arise that do not fit neatly within the remit of one particular department. Indeed, government departments might focus on one phase of what is actually a multi-layered risk management cycle...Policymakers, regulators and emergency services with narrow or short-sighted focus on achieving their individual mandates may also miss opportunities, fail to leverage the expertise of colleagues in different government departments, compare different types of risks and share lessons learned... (OECD 2009b, pp.4-5).*

Supply chain security initiatives that fail to encourage cross-agency communication and cooperation invite the same sort of costs and inefficiencies as initiatives that ignore the commercial aspects of the supply chain. The preferred governance model for risk management as identified by the OECD from its various case studies is therefore one that is characterised by an approach that addresses networked risk by:

- Coordinating the many central, regional and local government bodies in their various efforts to implement national policy goals related to public safety and security.
- Providing guidance to such bodies on how to conduct risk assessments.
- Streamlining and standardising reporting requirements for risk assessment and emergency management plans through a common information sharing mechanism (OECD 2009, p.11).

The WCO SAFE Framework with its Government-to-Business and Government-to-Government pillars is a good example of a governance approach that is relevant and effective in the international trade and transport security environment.

100 per cent scanning

As previously noted, the concept of 100 per cent scanning in the current environment represents the antithesis of risk management. Furthermore, social expectations no longer accept the concept of intervention for intervention's sake. Rather, the current catch-cry is *intervention by exception,* intervention when there is a legitimate need to do so, that is, intervention based on identified risk.

The 100 per cent scanning of containers cannot be considered to represent a risk-based regulatory control mechanism, as the absence of any form of selectivity excludes its qualification as a legitimate risk treatment. The CSI program, on the other hand, is selective in that it focuses on specific ports and adopts a risk-based targeting strategy within those ports. As noted by Straw (2008):

> *DHS has long asserted that it screens 100% of US-bound cargo containers. That never meant a physical examination of each container, however. Rather, it referred to a risk-based screening, beginning with a review of all US-bound container manifests at their ports of departure for information that indicated elevated risks. Only in cases where documentation gave reason to suspect elevated risk would a container be subjected to physical scanning or inspection.*

The rationale for attempting to scan 100 per cent of containers is also questioned by Ritter (2009), who comments:

> *...logic follows that there must be a direct relationship between quantity of scanning and risk mitigation. Unfortunately, a stronger relationship actually exists between risk mitigation and enhancing the quality of scanning. The global trade industry would be better served by focusing on mandating improvements in the type of cargo scanning rather than insisting that additional effort be focused on the quantity of scanning.*
>
> *The portal monitors have proven to be an ideal technology for verifying that legitimate radioactive cargo is present in the supply chain – but little more. Trucks continue to trigger alarms by the thousands per day, and secondary inspections are being performed with increased frequency in US ports and other select locations throughout the world. These secondary inspections ultimately serve to verify that commodities such as smoke detectors, fire brick, or cat litter are, in fact, emitting harmless amounts of radiation. But verifying normal is not the objective. And the actual utility of this approach, with regard to security threats, is still unclear.*

The policy to introduce 100 per cent scanning has, more than any other US strategy, caused significant global concern about the likely impact of such an initiative on the flow of maritime trade. US trading partners have previously accepted with little argument the introduction of similar initiatives such as CSI, but there has been an international backlash following this latest move. There are several reasons for this.

Firstly, 100 per cent scanning would have an unacceptable impact on trade, and the world is starting to question the need for such intrusive (in terms of business impact) strategies.

Secondly, an international transport environment that has for the past decade been striving to achieve an appropriate balance between trade facilitation and regulatory intervention sees this as a significant backward step. And thirdly, there is growing evidence to suggest that, for many economies, the primary objective in implementing the various security-related initiatives has little to do with the aim of minimising the occurrence and impact of terrorism, and is more concerned with maintaining a healthy trading relationship with US.[16] In this regard, the OECD notes that 'It is sometimes argued that many emerging security initiatives at ports outside the USA are driven by the fear that doing nothing will make it hard or impossible to export to the USA, not by security concerns as such. This incentive may compromise the effectiveness of the measures that are taken' (2009, p.13).

Observations on the 10+2 Rule

The ISF or 10+2 Rule is based on the same supply chain security philosophy as the Container Security Initiative, although in this case the initiative relates to the information associated with the cargo, in line with the 24-hour (Advance Manifest) Rule. In essence, it extends the Advance Manifest requirement further into the supply chain, at least from a data perspective, and shifts the 'virtual border' of the US beyond the port of loading of the cargo back to the manufacturer.

If the supply chain is examined from the perspective of CBP or other country equivalent and it is assumed that the US port of destination is the central node in the supply chain for a particular consignment, the data elements that comprise the ISF can be characterised as follows:

Upstream in the Supply Chain (Importer/Customs Broker)

- Manufacturer
- Seller
- Container stuffing location
- Consolidator
- Country of Origin
- HS classification

Upstream in the Supply Chain (Carrier)

- Vessel Stow Plan
- Container Status Message

Downstream in the Supply Chain (Importer/Customs Broker)

- Buyer
- Importer of Record
- 'Ship To' Party
- Consignee

The success or otherwise of the ISF as a risk management tool is totally dependent on its foundation, that is, the quality and timeliness of the data provided. If the data is false or

inaccurate, either intentionally or otherwise, the utility of ISF is compromised as are the risk decisions that flow from that data. In this regard, the '+ 2' component of ISF that is provided by the carrier does not really alter the risk equation because while the container is moving, there is less risk of illegal cargo being introduced to the container than when it is stationary (OECD 2005).

Any person or group that is intent on using the supply chain for criminal/terrorist activity is unlikely to advertise the fact through poor documentation of the trade and transport transaction. It is more probable that they will utilise legitimate sources and plausible data so as not to draw attention to the transaction. For example, they may set up a legitimate international trading company or purchase one and establish their legitimate trading credentials over a period of time. It is also likely that they may seek to use a well-known and established carrier or logistics provider, perhaps even one that is C-TPAT certified or a 'known shipper'. Anyone who may consider this scenario to be far-fetched need only refer to the example of the 'Khan Network' and the level of sophistication exhibited in that case.[17]

ISF is unlikely to detect anything unusual about a transaction in situations where the associated information has been constructed in such a way, and yet such a shipment logically falls at the 'Very High' or 'Extreme' end of the risk scale, at least as far as impact is concerned. If, on the other hand, the ISF data is inaccurate but not intentionally inaccurate (for example, transcription errors or some other carelessness), it is still unlikely to be detected by regulatory screeners, but more likely to be detected than a carefully constructed scam. An economist once argued, 'If Customs insisted on more accurate manifest reporting, it would be far easier to identify shipments that posed a security risk'. However, the authors do not recall anyone actually describing their cargo as 'weapons of mass destruction'!

Note also that investigations to uncover sophisticated illegal activities are extremely complex and take considerable time to complete, and consequently, targeting under the 24-hour Rule is completely reliant upon automated processing systems. For example, it took the authorities about ten years to uncover the activities of the Khan Network, and there is little doubt that such activities would not have been identified within 24 hours, even if the additional data elements required under the 10+2 Rule had been submitted.

Good intelligence and risk indicators based on that intelligence are currently, and are likely to remain the most effective and efficient means of detecting unlawful activity prior to arrival of a consignment. Requesting cargo-related information as early as possible in an international trade transaction provides extra time for border agencies to undertake a meaningful risk assessment of the cargo and decide whether or not to intervene, either by scanning, physical inspection or import prevention, but it should be emphasised that it is this temporal aspect of ISF rather than the data requirements themselves that is beneficial to the enforcement objective.

It is therefore considered that the ISF requirements add cost to an international trade transaction without commensurate benefit. A more cost-effective approach that is also more likely to identify supply chain security risk is through secure and 'real-time' access (that is, visibility on demand) to existing commercial data in the supply chain and the leveraging of partnerships with the private sector to assist in identifying anomalies. In the absence of specific intelligence such as evidence of an 'internal conspiracy', it should be recognised that industry participants are better placed than regulators to observe what is 'normal' and 'abnormal' as goods move along the supply chain.

Governments can add value by facilitating the process through appropriate regulation, international cooperation and harmonisation/standardisation so as to maximise supply chain visibility. Value is not added through the prescription of additional data requirements.[18] As noted by Laden, 'A good supply chain security program should retain the flexibility to achieve the goal of a more secure system of global trade...not simply become another "paper tiger" ' (2007, p.80).

A good example of the role that governments can play is in the closely related area of export controls. The publication and dissemination of 'Denied Persons Lists' and 'Red Flag' indicators to the public and private sectors provide guidance to supply chain participants concerning potential risks, and also serve to supplement supply chain visibility. A particular advantage of this approach to regulators such as Customs is that it treats the supply chain itself as an additional compliance management resource.

100 per cent scanning and 10+2 Rule in context

The 100 per cent scanning strategy and 10+2 Rule are intended to form part of the broader suite of security programs which include such initiatives as C-TPAT and AEO. These initiatives are in turn designed to provide Customs with a degree of confidence about the security of a participant's supply chain. This being the case, the question that must be asked is this: If a trader demonstrates a commitment to global supply chain security by achieving and maintaining AEO status, does there remain a genuinely risk-based need for the trader to provide advance information to the authorities who granted that status, and for their cargo to be scanned as a matter of routine?

This brings us back to Parker's (2000) description of compliance-orientated regulation, particularly the need to focus on the substantive objectives that the policymaker is seeking to achieve, and the extent to which the chosen regulatory regime is in fact able to achieve those objectives. As noted by Grainger, 'The challenge in reducing transaction costs and meeting regulatory control objectives – like those of increased security – is to consider how best to align the institutional framework with operational requirements' (2007, p.26).

Compliance assessment/regulation model

From a compliance perspective, regulated entities can generally be divided into three categories:

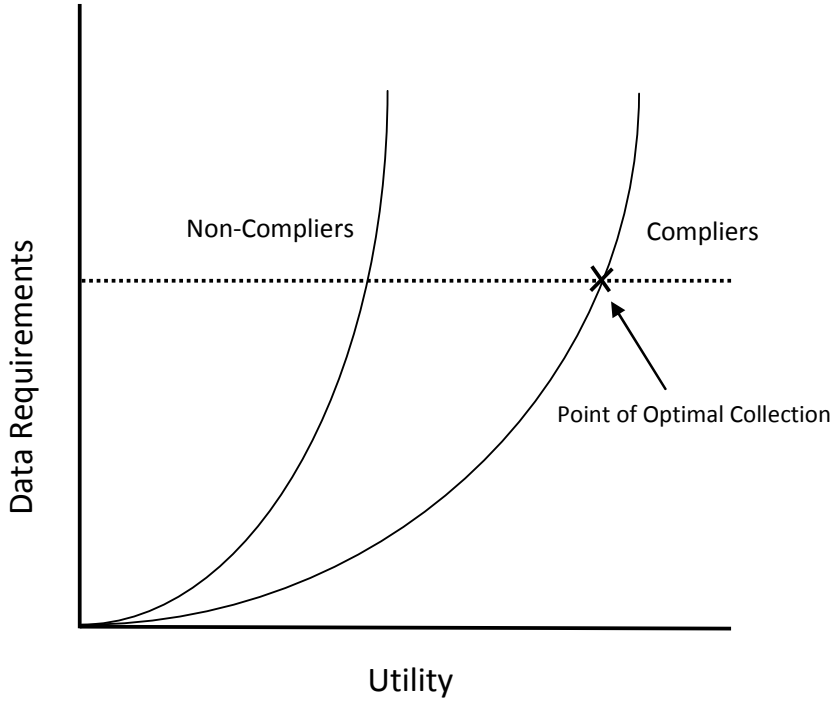
- Those who will actively seek to comply.
- Those who will comply provided they are given appropriate incentives to do so (including appropriate incentives to avoid non-compliance).
- Those who will intentionally pursue a course of non-compliance.

Compliant members of the international trading community (including those who fall into the second category) will generally provide Customs with accurate information in relation to their consignments. The information provided facilitates the identification of the cargo, the means of transportation and the various industry participants in the supply chain, and the fundamental data elements will provide Customs with a basic snapshot of the relevant consignment. While further data elements will assist in building a fairly comprehensive picture relatively quickly, there comes a saturation point at which additional information is unlikely to usefully contribute to the regulator's knowledge of the transaction.

Based on the assumption that deliberate non-compliers are unlikely to submit completely accurate information to Customs, the authors believe that the saturation point for such non-compliers will be reached much earlier in the data submission process. In other words, given that certain data elements will be inaccurate, Customs will at best have access to a handful of relevant information, and will be unable to develop a true picture of the transaction beyond some very basic aspects such as the vessel, carrier and the like. This is because non-compliers are unlikely to provide Customs with information that may attract attention from a risk-targeting perspective. This phenomenon is illustrated graphically in Figure 2.

Some may argue that profiling techniques are capable of identifying such situations. The reality is, however, that profiling is not a particularly successful technique for detecting sophisticated illegal activity of this nature. For example, Press argues that 'strong profiling (defined as screening at least in proportion to prior probability) is no more efficient than uniform random sampling of the entire population, because resources are wasted on the repeated screening of higher probability, but innocent, individuals'.[19]

Figure 2. **Compliance assessment/regulation model**



Source: Widdowson & Holloway (2009)

The model addresses the utility of routine data collection relating to individual transactions from the perspective of identifying potential regulatory non-compliance. It postulates three basic principles that can be summarised as follows:

- As data requirements increase, the value added to the assessment process decreases exponentially.

- Beyond a particular point (point of optimal collection) the requirement for additional information adds a regulatory burden to non-compliers with minimal benefit to the regulator.

- The point of optimal collection is reached earlier for non-compliers than for compliers.

The above model is qualitative in nature, and has not been tested by way of empirical research. The authors would encourage research that is designed to test the validity of the model.

Conclusions

International attempts to retrofit security regulation into already overly complex cross-border regulatory frameworks are resulting in particularly costly outcomes for industry, and this at a time when economic stimulation is supposedly high on the global political agenda.

Regulatory initiatives must therefore be carefully scrutinised to ensure that they are achieving a cost-effective outcome for both business and government that is consistent with:

- The desired policy outcome.

- The nature of the operational environment being regulated including both its commercial practices and relative security risks.

- The extent to which the regulatory requirements are likely to impact on the operational effectiveness of the activity being regulated, in this case international trade and transport.

In the authors' opinion, the approach that is most likely to achieve these objectives is one of compliance-orientated regulation in which the elements of both enforcement and incentives to comply with regulatory requirements are present in preference to a prescriptive approach that is likely to be less cost effective and more disruptive to commercial operations.

NOTES

1. See, for example, David Widdowson (2004), 'Managing risk in the customs context', in Luc De Wolf & José B. Sokol (eds), *Customs Modernization Handbook,* World Bank, Washington, DC, pp.91-99.

2. US Transport Safety Authority Known Shipper Program, accessed on 10 May 2009, www.tsa.gov

3. Case study taken from the *Mail on Sunday*, 18 August 2006, accessed 10 May 2009, www.bodine.phila.k12.pa.us/kaufman/ITGSweb/assignments/ipod/ipodchina.htm.

4. Event and exception management provides authorised individuals with notification of events that have an impact on the decision-making process. In the business context, this might be something like a shortage of inventory or shipment delay. In the government context, this might be a change in transport route, origin or company details. It can form an effective element of a profiling and targeting system.

5. See, for example, Alan Long (2009), 'Port community systems', *World Customs Journal,* vol. 3, no. 1, pp.63-67.

6. US Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (the Bioterrorism Act) which came into effect on 12 December 2003.

7. The Act requires registration of all domestic and foreign food facilities that manufacture/process, pack, or hold food for human or animal consumption in the US.

8. www.dhs.gov/xprevprot/programs/gc_1165872287564.shtm, accessed 15 May 2009.

9. American Shipper Magazine, 30 October 2008.

10. American Shipper Newswire, 30 October 2008.

11. Web Memo published by 'The Heritage Foundation', No. 1955, 13 June 2008.

12. Straw (2008).

13. Straw (2008).

14. Straw (2008).

15. Ritter (2009).

16. Author's interview with officials from twenty customs administrations.

17. See, for example, Crawford & Stecklow (2004), or Albright & Hinderstein (2005).

18. It should be noted that CBP has 'softened' its stance on ISF recently, for example, by showing restraint in enforcing the rule until March 2010, and relaxing some elements of interpretation and reporting timelines. However, the fundamental thrust of the initiative remains inappropriate in terms of risk management and commercial reality.

19. Proceedings of the National Academy of Sciences of the USA, www.pnas.org/cgi/doi/10.1073/pnas.0813202106.

REFERENCES

Aberdeen Group (2006), *Industry priorities for visibility, B2B collaboration, trade compliance, and risk management*, Global Supply Chain Benchmark Report, June, Boston, MA.

Albright, David and Corey Hinderstein, (2005), 'Unraveling the A.Q. Khan and future proliferation networks', *Washington Quarterly*, Spring, pp.111-128.

Bennear, Lori S. (2007), 'Are management-based regulations effective? Evidence from state pollution prevention programs', *Journal of Policy Analysis and Management,* vol. 26, no.2, pp.327-348.

Blegen, Bryce C. (2009), 'US importer security filing: advance electronic data under the SAFE Framework meets the real world', *World Customs Journal,* vol. 3, no. 1, pp.71-83.

Closs, D., C. Speier; J. Whipple, and M.D. Voss (2008), 'A framework for protecting your supply chain', *Supply Chain Management Review*, March.

Crawford, David and Steve Stecklow (2004), 'Supply chain: how the Pakistani nuclear wing managed to skirt export laws', *Wall Street Journal Online,* 23 March, at www.wsj.com.

Dahlman, O., J. Mackby, B. Sitt, A. Poucet, A. Meerburg, B. Massinon, E. Ifft, M. Asada and R. Alewine (2005), *Container security: a proposal for a comprehensive code of conduct*, January, National Defense University, Center for Technology and National Security Policy, Washington, DC.

European Commission (2007), 'Authorised Economic Operators: guidelines', Working Document TAXUD/2006/1450, EU, Brussels.

General Accounting Office (GAO, 2008), GAO-08-533T, *Supply chain security: challenges to scanning 100 percent of US-bound cargo containers*, 12 June, Washington, DC.

Grainger, A. (2007), 'Supply chain security: adding to a complex operational and institutional environment', *World Customs Journal,* vol. 1, no. 2, pp.17-29.

International Network for Environmental Compliance and Enforcement (INECE, 2009), *Principles of environmental compliance and enforcement handbook,* April, INECE, Washington, DC.

Laden, Michael D. (2007), 'The genesis of the US C-TPAT program: lessons learned and earned by the government and trade', *World Customs Journal,* vol. 1, no. 2, pp.75-80.

NetRegs (2003), 'SME-nvironment 2003 survey', accessed 10 May 2009, www.netregs.gov.uk/netregs/links/63809.aspx.

Organisation for Economic Co-operation and Development (OECD, 1997), *Report on regulatory reform: synthesis,* OECD, Paris.

Organisation for Economic Co-operation and Development (OECD, 2005), **'**Container transport security across modes', European Conference of Ministers of Transport, OECD Publishing, Paris.

Organisation for Economic Co-operation and Development (OECD, 2008), *Management-based regulation: implications for public policy*, GOV/PGC/REG(2008)5, Paris.

Organisation for Economic Co-operation and Development (OECD, 2009a), **'**Security, risk perception and cost-benefit analysis', Discussion Paper No. 2009-6, March 2009, Joint Transport Research Centre, International Transport Forum, Paris.

Organisation for Economic Co-operation and Development (OECD 2009b), *Innovation in country risk management*, OECD Studies in Risk Management, Paris.

Organisation for Economic Co-operation and Development (OECD, 2009c), 'Managing and improving compliance: recent developments in compliance risk treatments', Information Note, Forum on Tax Administration: Compliance Sub-Group, Centre for Tax Policy and Administration, March 2009, Paris.

Parker, Christine (2000), 'Reinventing regulation within the corporation: compliance-oriented regulatory innovation', *Administration & Society,* vol. 32, no. 5, pp.529-565.

Poole, Robert W. (2008), Toward risk-based aviation security, JTRC Discussion Paper 2008-23, www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200823.pdf.

Purtell, Dan and James B. Rice Jr. (2007), 'Assessing cargo supply risk', *Security Management Online,* 15 June, www.securitymanagement.com, accessed on 7 May 2009.

Ritter, Luke (2009), '100% cargo scanning mandate: quantity, quality and the optimal solution', Editorial, Homeland Security Innovation Association, www.hlsia.org.

Sarathy, Ravi (2005), 'Terrorism, security and the global supply chain', paper presented at the Conference on *International Trade and Logistics, Corporate Strategies and the Global Economy*, University of Le Havre, September 2005.

SITPRO (2008), *A UK review of security initiatives in international trade,* SITPRO, London.

Straw, Joseph (2008), 'Outlook for container scanning', October, www.securitymanagement.com.

Sweden National Board of Trade (2008), *Supply chain security initiatives: a trade facilitation perspective*, Stockholm, Sweden.

Tirschwell, Peter (2009), 'The truth about 10+2', *Journal of Commerce Online,* 16 February, www.joc.com/node/409178.

United Nations Conference on Trade and Development (UNCTAD, 2006), 'ICT solutions to facilitate trade at border crossings and in ports', Document TD/B/COM.3/EM.27/2, UNCTAD, Geneva.

Widdowson, David (1998), 'Managing compliance: more carrot, less stick', in Chris Evans & Abe Greenbaum (eds), *Tax administration: facing the challenges of the future,* Prospect, Sydney, pp.99-104.

Widdowson, David (2005), 'Customs partnerships: a two-way street', paper presented to the European Customs Conference organised by the European Forum for Foreign Trade, Customs and Excise, Bonn, Germany, 10 June.

Widdowson, David (2006), 'Raising the Portcullis', paper presented to the WCO Conference on Developing the Relationship between the WCO, Universities and Research Establishments, Brussels, March.

World Customs Organization (WCO, 2004), 'New trends in international trade, emerging business models, and the needs of small and medium-sized businesses in preparing the Framework of Standards to Secure and Facilitate Global Trade', WCO, Brussels.

World Customs Organization (WCO, 2007), *WCO SAFE Framework of standards to secure and facilitate global trade,* WCO, Brussels.

World Customs Organization (WCO, 2008), Customs in the 21st Century: Enhancing growth and development through trade facilitation and border security, WCO, Brussels.