



WORLD CUSTOMS ORGANIZATION

WCO Research Paper No. 3

The WCO SAFE Framework of Standards: Avoiding Excess in Global Supply Chain Security Policy

(November 2009)

Robert Ireland

Abstract

Prior to the terrorist attacks of 11 September 2001, customs controls related to national security threats did not feature highly on the policy priorities of the World Customs Organization (WCO). After 9/11 and implementation of several US Customs programs such as the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT), and regulations such as the 24-Hour Rule, the WCO began to focus much more of its work on supply chain security. This transition culminated in 2005 with the adoption of the WCO SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), a non-binding instrument comprised of technical customs standards aimed at securing without impeding international trade. This article will discuss the intricacies of the SAFE Framework including its history, political context, and technical elements (especially risk management and the Authorized Economic Operator (AEO) concept) and antecedents. This article will also consider the 2007 US legislation mandating 100% scanning of US-bound cargo containers at foreign ports that clouds and constrains the SAFE Framework's future. The article concludes that policymakers should seek to avoid excess in formulating supply chain security policies.

Key words

WCO SAFE Framework, supply chain security, AEO, 100% container scanning

Acknowledgements

This paper was written by Robert Ireland of the WCO's Research and Strategies Unit in the Office of the Secretary General. This paper was previously published in the *Global Trade and Customs Journal*. Cite as Ireland, Robert (2009), "The WCO SAFE Framework of Standards: Avoiding Excess in Global Supply Chain Security Policy," *Global Trade and Customs Journal* 4 (11/12). The author is grateful to Kunio Mikuriya, Christopher Kristensson, Raymond McDonagh, Mariya Polner, John Raven, Tadashi Yasui, and Jae-Young Choi for their suggestions.

Disclaimer

The WCO Research Paper Series disseminates the findings of work in progress to encourage the exchange of ideas about Customs issues. The views and opinions presented in this paper are those of the author and do not necessarily reflect the views or policies of the WCO or WCO Members.

Note

All WCO Research Papers are available on the WCO public website: www.wcoomd.org. The author may be contacted via communication@wcoomd.org.

Copyright © 2010 World Customs Organization.
All rights reserved.

Requests and enquiries concerning translation, reproduction and adaptation rights should be addressed to copyright@wcoomd.org.

1. INTRODUCTION

Before 11 September 2001, national security and anti-terrorism were not among the major roles and responsibilities of customs administrations worldwide.

In developed countries, most customs administrations targeted trade in illegal commodities, such as narcotics and counterfeit goods. Moreover, some governments were attempting to balance the inevitable speed bumps of frontier controls with the benefits of *trade facilitation*,¹ the concept that asserts customs and other border agency procedures should not unnecessarily slow legitimate trade with excessive formalities and regulatory zeal.

Most customs administrations in developing countries were concerned predominantly with levying and collecting duties and taxes because, unlike the developed nations where most public finance is derived from personal income tax, value added taxes, and other indirect taxes, customs duties in developing countries frequently fund a sizeable portion of government operations.

Regardless of these varying priorities, a common thread of the customs environment before 11 September 2001, was the emphasis, both theoretically and operationally, on the place of import (Mikuriya, 2007: 51). Whether deterring smuggling, reducing red tape at the border, or collecting customs duty, customs administrations generally concentrated on imports rather than exports and the focus of customs controls and analysis took place at the physical place of import or the premises of the trader rather than the other nodes along the supply chain.² Moreover, the World Customs Organization (WCO),³ the international body that represents customs administration interests, paid little attention to supply chain security and terrorism.

2. THE POST-9/11 SUPPLY CHAIN SECURITY PARADIGM

The violence of 9/11 changed these priorities, especially for the US Customs Service,⁴ the WCO, and many customs administrations in the developed world. Customs in developing countries continued to focus on revenue collection, but the new and acute security concerns had an impact on them as well.

Following the 9/11 attacks, cacophonous public and political discussions took place within the US on policy alternatives for security precautions for every conceivable

¹ Trade Facilitation has been defined as “the simplification and harmonization of international trade procedures” where trade procedures mean the “activities, practices and formalities in collecting, presenting, communicating and processing data required for the movement of goods in international trade.” As quoted in Grainger, Andrew (2007), *Trade Facilitation: A Review*: 4.

² An exception to this generalization was pre-shipment inspection (PSI), where a specialized business, hired by the government of the importing country, applied procedures at the time and place of export primarily for purposes of verification of classification, valuation, quality, and quantity of the traded goods.

³ The WCO is an intergovernmental organization based in Brussels, Belgium that develops international customs conventions, instruments, best practices, guidelines, and tools. The WCO’s members are customs administrations from around the world.

⁴ The US Customs Service became US Customs and Border Protection (CBP) on 1 March 2003, and shifted from the Department of Treasury to the new Department of Homeland Security (DHS).

threat and vulnerability. There was little deliberation about the expense or risks of a disproportionate response. Some commentators posited that international trade, especially when containerized, is an activity that can be exploited as a delivery mechanism for weapons of mass destruction (also known by its broad stroke acronym WMD), such as a 'nuke in the box' or 'dirty bomb.' Stephen E. Flynn, who has worked for the US Coast Guard, Science Applications International Corporation (SAIC), and the Council on Foreign Relations, rose to prominence as an alarm raiser about ocean-going cargo containers potentially being the Trojan Horse of the twenty-first century (Flynn, 2002: 60). For some policymakers and researchers, the risk of containers delivering deadly blows has had sustained validity.

And what are those blows, specifically? In essence they are based on the supposition that WMD, hidden within containers, could be unleashed to deliver catastrophic social and economic damage. A key customs task therefore became the prevention of this putative cataclysmic threat.

Defining terms or nomenclature is essential in devising, explaining, and justifying clear, efficient, and effective public policies. There are several definitions of WMD,⁵ but this article will rely on the United Nations, which adopted a formal definition in 1948 that has been used in a number of disarmament conventions:

atomic explosive weapons, radioactive material weapons, lethal chemical and biological weapons, and any weapons developed in the future which have characteristics comparable in destructive effect to those of the atomic bomb or other weapons mentioned above (UN, 1948).

Thus, the concept of WMD can reasonably be understood to include nuclear, radiological, biological, and chemical weapons that can cause massive damage to people by people. These four weapon types, however, are so dissimilar in ease of use, potential impact, and the appropriate response after dispersion that blending them together in one amalgamation is an oversimplification (Cote, 2003: 26-27). Government should accept and seek cognizance of these nuances when devising appropriate responses.

An important part of the analysis of the customs foray into national security are the three levels of customs controls that have been expounded upon by Martonosi, Ortiz and Willis (2006) – screening, scanning, and physical inspection. Martonosi et. al defines *screening* as “the initial assessment of the risk of a container based on the manifest, shipper, carrier, consignee and other information associated with the shipment” (Martonosi et. al., 2006: 220). *Scanning* is the imaging of containers using non-intrusive inspection equipment (NII) such as X-ray or gamma machines to evaluate whether any anomalies exist that would lead the customs officer to decide that physically inspecting the scanner by hand would be prudent. *Physical inspection* is the potentially lengthy and cumbersome process of customs officers opening a container and examining a sample or up to all of the contents by hand.

⁵ For a history of WMD nomenclature, see Carus, Seth W. (2006), *Defining Weapons of Mass Destruction*, Washington, DC: National Defense University Press.

In the 9/11 aftermath, US Customs, led by Commissioner Robert Bonner (2001–2005) swiftly implemented a number of new programs and policies that were aimed at preventing global trade, including container traffic, from being used as a conduit for terrorism. Most significantly, Mr. Bonner launched C-TPAT in 2001 and CSI in 2002. Both programs are still operational. In 2003, US Customs began enforcing the 24-Hour Rule, which requires sea carriers to provide US Customs with detailed descriptions of the contents of sea containers bound for the United States 24 hours before the container is loaded on board a vessel (frequently cargo destined for the US is first subject to feeder traffic before it is loaded on the container ship).

C-TPAT, the first security oriented customs Authorized Economic Operator (AEO) program, is a voluntary partnership between US Customs and international trade operators. In essence, businesses seeking to join C-TPAT are required to ensure the application of a specified list of minimum security measures along their supply chain. Once the package of measures is validated by US Customs, a business is entitled to various benefits, such as faster clearance time, reduced number of inspections, and reduced quantity of compliance measurement examinations. C-TPAT membership is open to businesses that are active in the US import supply chain, including US-based importers, carriers, port and terminal authorities, customs brokers, freight consolidators, and some foreign manufacturers.

CSI places US Customs officers at foreign ports to screen containerized cargo exported to the United States, with the aim of decreasing the possibility they could be used for transporting WMD. Although there are issues of sovereignty and reciprocity, requested countries agreed to host US Customs officers. In instances where the officers, using risk criteria to analyze data elements, identify cargo as being high-risk, they can request that the national customs administration scan or physically inspect the cargo. There is no guarantee, of course, that the host nation will agree to the request or that they will conduct a diligent inspection (Sapolsky, Gholz, and Talmadge, 2009: 147).

US Customs describes CSI as having three core imperatives: (1) “Identify high-risk containers. CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence. (2) Prescreen and evaluate containers before they are shipped.” Containers are screened as early in the supply chain as possible, generally at the port of departure. (3) Use large-scale X-ray and gamma ray machines and radiation detection technology to scan containers determined to be high risk (US Customs, 2008). Thus far, US Customs has not identified WMD in cargo shipped to the United States, and there have not been any attacks on US ports using WMD hidden in containers.

Under CSI and the 24-Hour Rule, all maritime containerized cargo bound for the United States is screened. Screened cargo that is determined to be high-risk is supposed to be scanned and perhaps physically inspected. The thrust of the US programs was and is that the screening of consignments and the scanning or physical inspection of high-risk consignments are required to happen long before arrival, essentially before they are loaded on the shipping vessel at the port of export.

From 2001 to 2006, the core construct of US policy on customs controls for national security was the use of risk assessment⁶ or selectivity. Using risk assessment, the customs administration analyzes consignment information to guide decisions on what shipments pose a high risk of non-compliance with customs laws or a security threat. Thus, the expressed purpose of customs risk analysis is to identify high-risk cargo and facilitate low-risk cargo.

The initial efforts to temper security with facilitation attempted to augment supply chain security at a reasonable cost, maintain cordial international relations, and minimize constraints on businesses trying to get their goods to market. Although expensive for both customs and the trade, CSI and C-TPAT cost less than some alternatives, such as 100% scanning or 100% physical inspection. All foreign governments were, publicly at least, amenable to allowing US Customs officers to work as observers at their ports. Businesses were promised benefits if they successfully joined C-TPAT. More radical approaches would have severely damaged free trade. In a pure security fortress model or neo-garrison state (Lasswell, 1941), a country could put all of its resources into homeland security and conceptually prevent anyone or anything from entering the country. That country would, however, be taking very uncomfortable decisions to shift government resources to unproductive investments, shoulder detrimental opportunity costs, and stifle their international trade.

In such circumstances, prudence suggests that full consideration should be given to the probability or risk of security fears being realized when devising the responses (Mueller, 2004). Moreover, careful and rational vetting should take place over whether it is worth allocating substantial resources rather than moderate resources to an unlikely event, when more likely events receive insufficient allocations.

In adopting security policies, a government should consider that eventually it will reach a point of diminishing marginal utility⁷ where the application of each additional unit of security regulation will yield smaller and smaller amounts of added security.

Some assert that excessive security can cause less safety (US GAO, 2008b: 6), and this could have some validity in the customs context. Undue customs controls without the filter of risk analysis can blunt and devalue the skills of customs officers and cause them to lose focus. Too much information can prevent a customs officer from evaluating or discovering what is important and what is not. Moreover, an overly rigid system can increase the potential for corruption; if the customs controls foment exceptional delays, traders may come under extra temptation to offer bribes to accelerate customs clearance and release.

⁶ Risk assessment in customs controls is a subset of the broader concept of customs risk management. The WCO has defined *risk management* as “the systematic application of management procedures and practices which provide customs with the necessary information to address movements or consignments which present a risk.” The WCO has defined *risk assessment* as “the systematic determination of risk management priorities by evaluating and comparing the level of risk against pre-determined standards, target risk levels or other criteria.” As quoted in WCO (2003b), *Risk Management Guide*.

⁷ Economist Hermann Heinrich Gossen is considered to be the original theorist of the general theory of marginal utility, as presented in his 1854 book *Die Entwicklung der Gesetze des menschlichen Verkehrs und der daraus fließenden Regeln für menschliches Handeln* (The Laws of Human Relations and the Rules of Human Action Derived Therefrom).

Ultimately, as political scientist Terry L. Deibel has said, policymakers should seek “not to counter all conceivable threats to the maximum degree, lest they do damage to other interests in the process (e.g., hurting prosperity by overspending to protect physical security) or generate counteractions that will leave interests less protected or advanced than when they began” (Deibel, 2007: 147).

3. THE WCO AND SUPPLY CHAIN SECURITY

On 26 June 2002, during its summit in Kananaskis, Canada, the G8 issued a statement called Cooperative G8 Action on Transport Security, which listed several policy steps in response to 9/11 on container security, aviation security, maritime security, and land transportation. In signalling that the starting gate was open for the development of a global supply chain security policy, the statement said, *inter alia*, that the G8 would:

work expeditiously, in cooperation with relevant international organizations, to develop and implement an improved global container security regime to identify and examine high-risk containers and ensure their in-transit integrity; develop, in collaboration with interested non-G8 countries, pilot projects that model an integrated container security regime; implement expeditiously, by 2005 wherever possible, common standards for electronic customs reporting, and work in the WCO to encourage the implementation of the same common standards by non-G8 countries; and begin work expeditiously within the G8 and the WCO to require advance electronic information pertaining to containers, including their location and transit, as early as possible in the trade chain (G8, 2002).

Also in June 2002, the WCO adopted a resolution that noted “the increased global concern with respect to acts of international terrorism ...” (WCO, 2002) and established a task force to develop instruments on securing and facilitating global trade. The WCO task force met six times and produced a package of technical measures, the most important of which, the Customs Guidelines on Integrated Supply Chain Management (ISCM Guidelines), embraces the application of risk assessment to an interoperable supply chain.⁸

Although the main thrust of the WCO task force was to be security, and though without 9/11 the task force would never have formed, it is instructive that they always paired ‘security’ with ‘facilitation.’ Proponents of trade facilitation, while conceding that customs controls are needed to deter illegitimate trade, seek to change the traditional relationship between customs and trader from regulator and the regulated, to procedural partners. In recognizing concerns expressed about the impact on trade facilitation, the WCO ensured there was a security and facilitation coupling (Mikuriya, 2007: 51). Thus, it is striking that what emerged was an agreement that strives for balance between security and facilitation with the assumption that a border agency can apply appropriate controls for purposes of security while minimizing border crossing obstacles for legitimate trade. This reflects the WCO’s view that, regardless of whether customs controls are for purposes of collecting customs duties or deterring illegal goods, by using risk assessment there should be and can be equilibrium between controls and trade facilitation. The notion that excessive controls without the use of systematic analysis

⁸ Standard 1 of the SAFE Framework is a commitment to follow the ISCM Guidelines.

make a customs administration less effective in applying the controls is well accepted within the customs community.

4. THE WCO SAFE FRAMEWORK

In an effort to raise the technical work of the WCO task force on security and facilitation to a prominent political level, the WCO established a High Level Strategic Group (HLSG) comprised of twelve WCO members. The HLSG met seven times from June 2004 to April 2007 and developed the WCO Framework of Standards to Secure and Facilitate Global Trade,⁹ which the WCO Council adopted in June 2005. Although not an international convention, the SAFE Framework is a set of voluntary standards to which most WCO Members have committed to pursue adherence. As of July 2009, 156 WCO members out of 174 had committed to implement the SAFE Framework.

Confidence in the efficacy of risk assessment is at the heart of the SAFE Framework, which draws on the contention that by analyzing risk, a customs administration can balance security controls with trade facilitation, and costs with benefits. The risk assessment ethos in customs security controls is that while every consignment should be screened, preferably at or before export, not all of them have to be scanned or physically inspected to increase security.

The SAFE Framework is organized into twin pillars, the first being customs-customs network arrangements and the second being customs-business partnerships. The total number of standards is seventeen, with eleven in Pillar 1 and six in Pillar 2.

Pillar 1 provides for the ability of a customs administration to receive the essential control data on exports, imports, or goods in transit in advance and electronically; analysis of the information to determine whether the shipment is high-risk in terms of national security; and scrutiny of high-risk consignments, preferably using nonintrusive inspection (NII) techniques. The facilitative aspect of this process is that a shipment deemed to be low-risk need not be scanned or physically inspected.

Pillar 2 builds on Pillar 1 with a recommended process where customs administrations validate as AEOs businesses that comply with security requirements and whose cargo would, therefore, generally be deemed low-risk under the procedures of Pillar 1. The SAFE Framework defines an AEO as:

a party involved in the international movement of goods in whatever function that has been approved by or on behalf of a national Customs administration as complying with WCO or equivalent supply chain security standards. [AEOs] include *inter alia* manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors (WCO, 2005).

Although the SAFE AEO relates to operators in the context of supply chain security, the intellectual precedent comes from the WCO's *International Convention on the Simplification and Harmonization of Customs Procedures*, also known as the revised

⁹ The instrument was later renamed the SAFE Framework of Standards to Secure and Facilitate Global Trade. SAFE stands for Security and Facilitation in a global Environment.

Kyoto Convention, which was adopted in 1973 and revised in 1999. The revised Kyoto Convention stipulates the following:

For authorized persons who meet criteria specified by the Customs, including having an appropriate record of compliance with Customs requirements and a satisfactory system for managing their commercial records, the Customs shall provide for:

- release of the goods on the provision of the minimum information necessary to identify the goods and permit the subsequent completion of the final Goods declaration;
- clearance of the goods at the declarant's premises or another place authorized by the Customs; and, in addition, to the extent possible, other special procedures such as;
- allowing a single Goods declaration for all imports or exports in a given period where goods are imported or exported frequently by the same person; (WCO, 1973)

One way of explaining the substance of the SAFE Framework is to divide it into four core elements, which are (1) a commitment to harmonize advance electronic cargo information requirements on imports, exports, and goods in transit; (2) the application of a consistent risk assessment approach for screening containerized cargo to identify potential security threats; (3) at the reasonable request of the country of import, the country of export will perform an examination of outbound high-risk containerized cargo preferably using NII, based on a comparable risk targeting methodology; and (4) the establishment of AEO programs where customs, upon successful validation or authorization of international trade operators who meet stipulated supply chain security standards and best practices, will grant trade facilitation benefits.

A close reader of this article will note that the SAFE Framework's Pillar 1 and Pillar 2 contents are not unfamiliar. This is because Pillar 1 can be interpreted as a globalized version of CSI, and Pillar 2 can be interpreted as a globalized version of C-TPAT (US GAO, 2008a: 7). Pillar 1 also draws from WCO instruments, especially the revised Kyoto Convention, the Immediate Release Guidelines, and ISCM Guidelines. Like Pillar 1, the revised Kyoto Convention embraces risk assessment as the central principle of a modern customs administration. Pillar 2 has its roots in the previously mentioned authorized person concept contained within the revised Kyoto Convention and *trusted trader* programs where customs administrations grant benefits to businesses that are regularly compliant with customs regulations or designated criteria as determined by risk assessment.

Because of the technical complexity and financial requirements, many WCO members are by necessity pursuing phased implementation of the SAFE Framework. To assist with that endeavor, the WCO and other organizations provide capacity building to assist WCO members from developing countries implement the SAFE Framework.

5. THE SAFE FRAMEWORK AEO AND AEO MUTUAL RECOGNITION

In 2006 the WCO, working with its trade partners, developed a new section within the SAFE Framework called AEO Conditions, Requirements, and Benefits, to further

develop the AEO concept. This new section provides more detailed information on how to establish an AEO program, especially the conditions and requirements for customs, the process by which customs should validate and authorize AEOs, and the benefits that should be provided to AEOs (Mikuriya, 2007).

A fragmented and disparate system of AEO programs will inevitably bring confusion to supply chain security efforts and consternation to business sensitivities. International trade operators seek uniformity so that their information technology systems do not need constant adjustment. In an effort to expand the AEO network, some customs administrations are making progress in pursuing mutual recognition of AEO programs by negotiating formal Mutual Recognition Agreements or Arrangements (MRA). Indeed, many customs administrations see mutual recognition as the primary reason to establish an AEO program.

Optimally, MRAs should provide mutual recognition of status (Irish, 2009) in that businesses of one AEO program are entitled to receive benefits identical or comparable to those conferred to businesses participating in another AEO program (US-EU JCCC, 2009). To agree on mutual recognition, the AEO programs must encompass compatible requirements; guidance on compatibility is presented in the SAFE Framework. Thus far, all concluded AEO MRAs are bilateral (Polner, 2009).

6. US LEGISLATION ON 100% SCANNING

In 2006, the US Congress began shifting the US away from risk assessment being at the centre of the supply chain security policies initiated in 2001, with unknown consequences for the future of the international trade system.

On 13 October 2006, the US enacted *The Security and Accountability for Every (SAFE) Port Act (The SAFE Port Act of 2006)*, which, *inter alia*, (1) codified in law CSI and C-TPAT; (2) required testing the feasibility of scanning all US-bound cargo containers; and (3) required scanning of all containers for radiation at the 22 busiest US ports (US CRS, 2006: 45-47). The US Department of Energy and US Customs then set up the Secure Freight Initiative (SFI), a pilot that required 100% scanning of US bound cargo at three ports and more limited scanning at four other ports. The purpose of the pilots was to evaluate the feasibility of scanning all cargo bound for the United States. Before the pilots could be completed and the results studied, however, the US made a U-turn away from risk assessment.

On 3 August 2007, the US enacted *The Implementing Recommendations of the 9/11 Commission Act of 2007*, which, *inter alia*, required that by July 2012 “a container that was loaded on a vessel in a foreign port shall not enter the United States (either directly or via a foreign port) unless the container was scanned by non-intrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel” (US Public Law 110-153, 2007).

The 2004 report of the *National Commission on Terrorist Attacks Upon the United States (9/11 Commission)* had not called for 100% scanning and in fact advocated risk assessment:

Hard choices must be made in allocating limited resources. The U.S. government should identify and evaluate the transportation assets that need

to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort (US National Commission on Terrorist Attacks Upon the United States, 2004: 391).

Under the 100 percent scanning regulation, however, the use of risk assessment would no longer be relevant because estimating the risk level of containerized cargo shipping would be purposeless as cargo containers, whether deemed high-risk or low-risk, are required to be scanned. This would conflict with the emphasis on using risk assessment in supply chain security controls. Accordingly, the law poses grave danger for trade facilitation and as a precedent for other non-facilitative measures.

Since the legislation's enactment, the WCO has actively lobbied the US Congress against 100% scanning. In December 2007, the WCO's Policy Commission issued a Resolution in Almaty, Kazakhstan, expressing its concerns at the US legislation. At the June 2008 WCO Council Sessions, the WCO membership endorsed the Almaty Resolution, which states that 100% scanning would be "detrimental to world trade," "would introduce a significant nontariff trade barrier," and "would deviate from trade facilitation and logistical efficiency and result in unreasonable delays, increased storage demands and port congestion ..." (WCO, 2007). In a speech at the EastWest Institute's 6th Worldwide Security Conference that took place in Brussels, Belgium in February 2009, the WCO Secretary General, Kunio Mikuriya, stated:

It is well understood that scarce resources need to be targeted at the higher end of the risk continuum. From this point of view the customs community has expressed its concern on the US legislation that requires 100% scanning of US-bound containers and is asking the US Congress to review the legislation. We believe that 100% scanning is not equal to 100% security and instead advocate a more risk-based approach (Mikuriya, 2009).

The law has caused consternation for business interests as well. The trading community, a lobbying group called the Safe Commerce Coalition (which is led by a former US Department of Homeland Security official and consists of businesses actively engaged in international trade), and the Heritage Foundation (a conservative think tank based in the United States), have also been vocal in opposition.

While recognizing that it is the law, US Customs has expressed concern as well. In an April 2008 speech, then US Customs Commissioner W. Ralph Basham (2005–2009) said:

scanning all 11.5 million containers that enter U.S. seaports at a foreign port presents significant operational, technical, and diplomatic challenges, including: sustaining the scanning equipment in extreme weather conditions and certain port environments; identifying who will incur the costs for operating and maintaining the scanning equipment; acquiring necessary trade data prior to processing containers through the SFI system; addressing data privacy concerns in regards to the scanning data; [and] staffing implications for both the foreign customs service and terminal operator (Basham, 2008).

Governments in developed and developing countries continue to criticize the policy, especially on trade barrier and expense grounds. Two prominent governmental

critics are a grouping of countries in Latin America (Bolivia, Cuba, the Dominican Republic, Ecuador, and Uruguay) and the European Commission (EC). In June 2009, Ecuador submitted a position paper that stated “100% scanning will also require a major re-structuring of ports, including a redistribution of maritime transport worldwide, and place a very heavy financial burden on business and taxpayers of all countries exporting to the US, especially on developing and least developed countries” (Embassy of Ecuador to the Kingdom of Belgium, 2009). In a July 2009 report, the EC said:

For the EU and other major partners, the envisaged scanning of all U.S.-bound containers in more than 600 ports from which ships leave for the U.S. would lead to major trade disruptions and an additional administrative burden. It would require major re-structuring of EU ports and place a very heavy financial burden on EU business and ultimately its taxpayers. The [U.S. legislation] does not include a spending authorisation/financial clause for equipping foreign ports. Therefore costs for the installation of the necessary equipment are expected to be borne by the port and shipping companies. An indication of the potentially devastating economic impact was provided by the pilot programme in the context of the U.S. Secure Freight Initiative (SFI) that was intended to evaluate the feasibility of 100% scanning and to install such full scanning equipment in seven international ports. It appropriated roughly \$60 million to cover costs in some, although not in all of the ports. For the Southampton pilot alone the costs were estimated at \$14.5 million (European Commission, 2009: 8).

In a 2008 report, the US Government Accountability Office (GAO), which is the investigative arm of the US Congress, identified nine challenges to the practical implementation of the SAFE Port Act and the 100% scanning requirement. Notably the GAO identified inconsistency with risk assessment, potential retaliation by reciprocity in that US trading partners may follow suit by requiring all cargo exported from the US be scanned, and the failure within the legislation to specify who would pay the inordinate amounts of money needed to purchase, use, and maintain the scanning technology (US GAO, 2008a).

7. SUPPLY CHAIN SECURITY POLICY ANALYSIS

This article has considered several parameters for the formulation of post-9/11 supply chain security policies including (1) which of the three aforementioned customs controls outlined by Martonosi, et. al. (2006) (screening, scanning, or physical inspection) should be emphasized;¹⁰ (2) whether to use pre-9/11 traditional risk assessment, post-9/11 security risk assessment aimed at the threat of containerized cargo delivering nuclear, radiological, biological, or chemical weapons, or to not use risk assessment; (3) whether the controls should be applied close to the time and place of import or close to the time and place of export; and (4) whether to establish an AEO security program. In analyzing the range of possibilities created by decisions for each of these four parameters, multiple theoretical options can be identified. Some of the

¹⁰ This assumes that these three activities can be escalated in one direction – screening can lead to scanning and/or physical inspection, and scanning can lead to physical inspection. Physical inspection cannot lead to scanning or screening and scanning cannot lead to screening. In addition, this article posits that ‘emphasis’ in this context means 100% or almost 100% screening or scanning or physical inspection.

theoretical options are not feasible; for example, it is not possible to conduct screening of containerized cargo without risk assessment.

To reduce the number of new policy options to a manageable level within this model, this analysis makes the following assumptions: (1) in applying customs controls for purposes of security, risk assessment is used in the context of a screening emphasis or no form of risk assessment is used in the context of a scanning or physical inspection emphasis;¹¹ (2) that currently there is a general consensus among most customs experts that the application of security controls should be conducted close to the time and place of export rather than close to the time and place of import; and (3) that there is a general consensus among most customs experts that establishing a security AEO program is a worthy objective as a complement to risk assessment but that it would be irrelevant in the context of a scanning or physical inspection emphasis.

In considering the above assumptions, this article posits that four broad policy options were conceptually available to regulators in their response to the perceived threats to the security of the international supply chain: (1) screening of all cargo containers using security risk assessment (and scanning and/or physical inspection of high-risk cargo) close to the time and place of export, and combined with an AEO security program; (2) scanning of all cargo containers with no risk assessment and close to the time and place of export; (3) physical inspection of all cargo containers with no risk assessment close to the time and place of export; and (4) the status quo, which in the pre-9/11 environment would entail customs, continuing to use risk assessment to determine the level of controls close to the time and place of import, using risk criteria linked to the pre-9/11 compliance concerns, such as narcotics, counterfeit goods, and commercial fraud. In addition, customs would use a revised Kyoto Convention 'authorized persons' program, not a security AEO program.

In conducting policy analysis, selection or evaluation criteria should be established to compare, measure, and select among alternative options. Cost, effectiveness, efficiency, and political feasibility are commonly used measures (Patton and Sawicki, 1993: 57). Although a case could be made for its effectiveness and efficiency, and certainly it would be low-cost compared to the alternatives, the status quo option was politically infeasible within the United States and other countries shocked by the 9/11 maelstrom and subsequent terrorist attacks elsewhere. The second and third options pose problems especially from effectiveness, efficiency, and cost perspectives, but also from a political feasibility standpoint internationally. Moreover, these options would increase risks and make 1930s protectionism look like child's play.

The first option, the SAFE Framework, was likely the most compelling choice for most stakeholders, especially in terms of political feasibility, but it also presented advantages on cost (except when compared with the status quo), effectiveness, and efficiency.

¹¹ Random controls would be another possibility, but for purposes of building a simple model and because this method never became part of the debate, it has not been considered here.

8. CONCLUSION

Avoiding excess in global supply chain security policy is essential to facilitate international trade; foster calm, productive and equitable international relations; enable beneficial allocation of scarce resources; and prevent excessive spending that merely achieves diminishing marginal utility or less security. This approach should be guided by empirical rather than anecdotal evidence; precise definitions of terms; consideration of probabilities; and the application of risk assessment principles to customs controls.

The WCO's SAFE Framework emerged as the global community's consensual policy choice for supply chain security in the post-9/11 environment. In 2006, however, 100% scanning of cargo containers with no risk assessment appeared in the US as a competing alternative to the SAFE Framework and its principle of risk assessment. Time will tell which option will ultimately prevail, or if a new political context will bring another option to the fore.

Bibliography

Basham, Ralph W. (2008), *Remarks Delivered by U.S. CBP Commissioner at National Customs Brokers and Forwarders Association of America Conference at Lake Buena Vista, Florida, 9 April 2008*, available at <www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/ncbfaa.xml>.

Carus, Seth W. (2006), *Defining 'Weapons of Mass Destruction,'* Washington, DC: National Defense University Press.

Cote Jr., Owen R. (2003), 'Weapons of Mass Confusion,' *Boston Review* 29, No. 29.

Deibel, Terry L. (2007), *Foreign Affairs Strategy – Logic for American Statecraft*, New York: Cambridge University Press.

Embassy of Ecuador to the Kingdom to Belgium (2009), *Position Paper on the SAFE Framework and the consequences of the United States law – 100% scanning*, submitted to the WCO on 26 June 2009.

European Commission (2009), *United States Barriers to Trade and Investment Report for 2008*, available at <trade.ec.europa.eu/doclib/docs/2009/july/tradoc_144160.pdf>.

Flynn, Stephen E. (2002), 'America the Vulnerable,' *Foreign Affairs* 81, No. 1.

Friedman, Benjamin H. and Harvey M. Sapolsky (2006), 'You Never Know(ism),' *Breakthroughs* XV, No. 1.

Grainger, Andrew (2007), *Trade Facilitation: A Review*, available at www.tradefacilitation.co.uk/content/view/17/39/>.

G8 (2002), *Cooperative G8 Action on Transport Security*, Kananaskis Summit, available at <www.g8.utoronto.ca/summit/2002kananaskis/transport.html>.

Irish, Maureen (2009), 'Supply Chain Security Programs and Border Administration,' *World Customs Journal* 3, No. 2.

Kunreuther, Howard (2001), 'Risk Analysis and Risk Management in an Uncertain World,' *Financial Institutions Center*, The Wharton School, University of Pennsylvania.

Lasswell, Harold (1941), 'The Garrison State.' *The American Journal of Sociology* 46: 455–68.

Levinson, Marc (2006), *The Box – How the Shipping Container Made the World Smaller and the World Economy Bigger*, Princeton: Princeton University Press.

Martonosi, Susan E., David S. Ortiz, and Henry H. Willis (2006), 'Evaluating the Viability of 100 Percent Container Inspection at America's Ports,' in Richardson, H.W., P. Gordon, and J.E. Moore (eds.) (2006), *The Economic Impacts of Terrorist Attacks*, Northampton, MA: Edward Elgar Publishing, 2006.

Mikuriya, Kunio (2003), *The Challenges of Facilitating the Flow of Commerce in a Heightened Security Environment*, in Cosgrave-Sacks, Carol and Mario Apostolov (eds.) (2003), *Trade Facilitation – The Challenges for Growth and Development*, UNECE.

Mikuriya, Kunio (2006), 'The Customs Response to the 21st Century,' *Global Trade and Customs Journal* 1, No. 1.

Mikuriya, Kunio (2007), 'Supply Chain Security: The Customs Community's Response,' *World Customs Journal* 1, No. 2.

Mikuriya, Kunio (2009), *Remarks Delivered by WCO Secretary General at the EastWest Institute 6th Worldwide Security Conference in Brussels, Belgium*, 18 February 2009, available at <[www.wcoomd.org/speeches/?v= 1&lid=1&cid=11&id=130](http://www.wcoomd.org/speeches/?v=1&lid=1&cid=11&id=130)>.

Mueller, John (2004), 'A False Sense of Insecurity?,' *Regulation* 27, No. 3.

Patton, Carl V. and David S. Sawicki (1993), *Basic Methods of Policy Analysis and Planning*, Englewood Cliffs, NJ: Prentice Hall.

Polner, Mariya (2009), *A Survey of Authorized Economic Operator (AEO) Programmes*, World Customs Organization Working Paper.

Raven, John (2001), '*Terrorism and Trade Facilitation*,' Working Paper, World Bank, Transport Web Library.

Raven, John (2005), *A Trade and Transport Facilitation Toolkit – Audit, Analysis and Remedial Action*, Washington, DC: World Bank.

Raven, John (2008), 'Security and Facilitation, the Two Scenarios,' *WCO News* No. 55.

Sapolsky, Harvey M., Eugene Gholz, and Caitlin Talmadge (2008), *US Defense Politics: The Origins of Security Policy*, New York: Routledge.

Sunstein, Cass R. (2005), *Laws of Fear – Beyond the Precautionary Principle*, New York: Cambridge University Press.

UN Commission for Conventional Armaments (1948), UN document S/C.3/32/Rev.1, in United Nations, Office of Public Information, *The United Nations and Disarmament, 1945–1965*, UN Publication 67.I.8, 28.

U.S. Congressional Research Service (2006), *9/11 Commission Recommendations: Implementation Status*.

U.S. Public Law 109 – 347 (2006), *Security and Accountability for Every Port Act of 2006* or the *SAFE Port Act*.

U.S. Public Law 110 – 53 (2007), *Implementing Recommendations of the 9/11 Commission Act of 2007*, Section 1701.

U.S. National Commission on Terrorist Attacks Upon the United States (2004), *The 9/11 Commission Report*.

U.S. Customs and Border Protection (2008), *CSI In Brief*, available at <www.cbp.gov/xp/cgov/trade/cargo_security/csi/csi_in_brief.xml>.

U.S. Government Accountability Office (2008a), *Supply Chain Security – Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers*, GAO-08-533T.

U.S. Government Accountability Office (2008b), *Supply Chain Security – CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain*, GAO-08-538.

US-EU JCCC (2009), *Abridged External Partner Version of the U.S.-EU Joint Customs Cooperation Committee Roadmap Towards Mutual Recognition of Trade Partnership Programs*.

WCO (1973), *International Convention on the Simplification and Harmonization of Customs Procedures (Revised Kyoto Convention, 1999)*.

WCO (2002), *Resolution of the Customs Co-operation Council on Security and Facilitation of the International Trade Supply Chain*.

WCO (2003a), *Guidelines for the Immediate Release of Consignments by Customs (Immediate Release Guidelines)*.

WCO (2003b), *Risk Management Guide*.

WCO (2004), *Customs Guidelines on Integrated Supply Chain Management (ISCM Guidelines)*.

WCO (2005), *SAFE Framework of Standards to Secure and Facilitate Global Trade (revised 2007)*.

WCO (2007), *Joint Resolution of the Customs Co-operation Council's Policy Commission and the Private Sector Consultative Group Concerning the WCO SAFE Framework of Standards and the United States Legal Requirements for 100 Percent Container Scanning at Export (Almaty Resolution)*.