57970

SUPPLY CHAIN SECURITY GUIDE

Michel Donner

Cornelis Kruk

The Transport Research Support program is a joint World Bank/ DFID initiative focusing on emerging issues in the transport sector. Its goal is to generate knowledge in high priority areas of the transport sector and to disseminate to practitioners and decision-makers in developing countries.

Supply Chain Security Guide

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org
E-mail: feedback@worldbank.org

CONTENT

List of Tables

List of Figures

List of Boxes

Foreword

In 2005 the World Bank decided to carry out a review entitled: "Review of the Cost of Compliance with the New International Freight Transport Security Requirements". The final report was published in February 2008. This report investigated the financial consequences of the introduction of the International Ship and Port Facility Security (ISPS) Code of the International Maritime Organization on the costs of cargo handling in ports.

During field investigations in Eastern Europe, Latin and Central America and West Africa, it appeared that there was a relatively good knowledge about the objectives and requirements of ISPS. But, at the same time, it also became clear that there was very limited knowledge about supply chain security (SCS), of which ISPS is one of the many components.

As SCS came more and more in the spotlight in international freight transport, this issue was discussed with a number of SCS experts and it was recognized that it would be advisable to increase SCS awareness in particular in port and trade facilitation communities in developing countries. The World Bank then embarked on the production of the present Supply Chain Security Guide.

The guide addresses the following main topics:

- What is supply chain security?
- Is it important to know about it?
- Who are the principal players / initiators?
- What are ports and logistic operators required to know or do so as to be ready when the SCS initiative compliance becomes globally compulsory?
- What is likely to happen in the field of SCS in the coming period of time?
- What is the expected end vision?

We hope that this Supply Chain Security Guide will be a useful tool and reference for all its readers, and we would like to express our gratitude to all the experts who have provided their time and expertise to finally produce this publication.

Marc Juhel
Sector Manager, Transport
The World Bank

Acknowledgements

The Supply Chain Security Guide was elaborated and published through the Transport Research Program, a financing of **DFID**, the Department for International Development of the United Kingdom Government.

We wish to express special thanks to Mr. Ger Diepens, World Customs Organization, WCO, Mrs. Jacqueline Dubow, World Bank Consultant, Mr. Jurjen Duintjer, Sohar Industrial Port Company, Mr. Gerard McLinden, Senior Trade Facilitation Specialist, World Bank, Mr. Kunio Mikuriya, Secretary General WCO, Mr. Peter Mollema, Port of Rotterdam Authority, Mr. Pascal Ollivier, Soget, Mrs. Anna Piasecka, World Bank, Knowledge Management Analyst, Mr. Jose Perrot, Port Autonome du Havre, Mrs. Helene Stephan, World Bank, Program Assistant, Mr. Michel Zarnowiecki, World Bank Consultant/Customs Specialist.

We would like to express our thanks to COTECNA Inspection SA which was contracted to provide the framework and technical contents of the guide, with principal contributions coming from William Boley and Mark Miller. Additional expertise was provided by Juha Hintsa and Baris Bicimseven from the Cross-Border Research Association.

Executive Summary

The tragic events of September 11, 2001, triggered a legitimate renewed focus on the security aspect of Trade and Transport-related matters. The most visible initiatives in this area have been:

- In 2001, the Customs-Trade Partnership Against Terrorism (C-TPAT) voluntary certification program (USA)
- In 2003, the implementation of the "24hr advanced manifest rule" for shipments to US ports
- In 2004, the implementation of the International Ship and Port Facility Security Code (ISPS Code) addressing the port and vessel segments of the maritime trade and transport security.

In 2005, the World Customs Organization (WCO) published its "Framework of Standards to Secure and Facilitate Global Trade". To date, 156 WCO Members have signed a letter of intent to implement the Framework. With such a heavy-weight prime mover, it is likely that the Framework of Standards will shape the majority of the future national supply chain security programs.

But these are only the visible part of the iceberg. When attempting to map out the current status of supply chain security, analysts find themselves confronted with a mosaic of "initiatives", programs, codes, "solutions", technological applications, regulations, which may be international, national, regional, sectoral, compulsory, voluntary, unilateral, bilateral, multilateral, mutually complementary or overlapping.

Non-specialists can legitimately become perplexed by the fluctuating and complex nature of the issue. Choosing the right orientations and making the right decisions while planning one's certification against such an evolving and dynamic background may leave many executives somewhat puzzled.

The same goes when one has to prepare for compliance to mandatory programs.

The multi-layered approach

The generally accepted trend calls for a layered approach, made of essential regulatory, conceptual, technological, programmatic and procedural components. More specifically, the main SCS elements are:

- Advance (electronic) Cargo Information (ACI)
- Risk Management
- Non-Intrusive Inspection (NII)
- Operators' Certification (Authorized Economic Operator - AEO)

The variety of programs that compose the layered approach are mutually complementing and even sometimes slightly overlapping each other in such a way that is meant to reinforce the whole structure:

- The ACI programs capture cargo information at an early stage, allowing the concerned Government Agencies to screen and analyze them through robust risk management techniques.
- The certification or credentialing programs aim at ensuring that supply chain actors are proven to be legitimate, self-disciplined and trustworthy.
- The application of recent technologies to SCS themes is being developed. For example: scanning and radiation detection, RFID-based "e-seals" and GPS-based container tracking,

computer-based data-analysis and targeting systems, designed to screen and interpret the mass of cargo data supplied every day by the ACI programs.

- The ISPS code and the ship-tracking systems cover the port-vessel interface and the ocean-leg of the voyage at vessel level. The ISPS code provides for the security norms for port installations.

However a number of variances and discordant sounds can be heard.

Compulsory or voluntary?

- The ACI programs, the ISPS Code and the vessel tracking systems are compulsory. The latter are globally compulsory for IMO Member States, the former are compulsory on the specific trade route they are regulating.
- While most AEO certification programs are not (yet?) compulsory, an increasing market- and peer-pressure is and will be felt by the supply chain actors, mainly exporters, importers and logistics operators, to become certified. Since AEO-certified operators must ensure that their vendors, subcontractors and trade-partners are themselves implementing adequate security measures, it will become more and more commercially risky **not to be certified**.

As the European Shippers Council (ESC) puts it, these voluntary programs are becoming "mandatory by default or design"[1].

The carrot takes the shape of privileged "green lane" treatment of certified operators' cargoes at border-crossing point, materialized by faster clearance and less frequent inspections.

Mutual recognition

It is generally agreed that there is a compelling case in favor of the international mutual recognition and interoperability between national AEO programs. The WCO Framework of Standards provides a common platform for AEO certification programs, which should facilitate their mutual recognition. There are, however, still some questions on the mutual recognition between C-TPAT and WCO-inspired AEO certification programs.

Capacity building

One notable initiative conducted by WCO is the Columbus Program, which is dedicated to the capacity building of Customs Administrations in support of the implementation of the Framework of Standards. This major effort might have been partly inspired by the difficulties met in many countries during the implementation of the ISPS code, and should contribute greatly to the implementation of the WCO Framework of Standards world-wide.

100% scanning

A bill was passed in the US in 2007, under the title "Implementing Recommendations of the United States 9/11 Commission Act of 2007", mandating overseas radiation scanning and NII inspection of 100% of all cargo containers destined for the U.S. by 2012. The word "overseas" contains a dimension of extraterritoriality that might be the stumbling stone of the so-called "100% scanning" program. On the other hand, it is already a law

[1] F.Beckers, Chairman, ESC "Shippers views on the directions of SCS legislation", May 2009 IAPH Conference

in one of the major players in international trade, even if its enforcement date has been set in the, not too distant, future.

Many analysts and observers consider that this initiative is running at cross-purposes with the prevailing multi-layered approach inasmuch as:

- It is contrary to the strategy of risk management and targeting of high-risk shipments, which enables the Government Agencies to allocate their limited resources to the areas where they are most needed.
- Given limited resources, 100% scanning may actually end up providing a lower level of security as the focused attention on specific high-risk shipments is being diluted and diverted to a "blanket" approach covering ALL containers, if customs officers are diverted from focusing on high-risk container cargo. "*Under the current risk-management system, for example, the scanned images of high-risk containers are to be reviewed in a very detailed manner. However, according to WCO and industry officials, if all containers are to be scanned, the reviews may not be as thorough*"[2].
- Its systematic approach might, paradoxically, give a delusive sense of security, whereas many specialists contend that truly high-risk shipments will actually receive less specific attention.

Other concerns relate to:

- The impact on the productivity of the ports and shipping industries and infrastructure, in general.
- The ability of the USA to reciprocate, should trade partners demand reciprocity
- The adoption of similar reciprocal exigencies by the other main global trade partners: BRIC (Brazil, Russia, India and China), EU, ASEAN+3, which would mean applying 100% scanning at origin *de facto* to the whole world
- The potential distortion of existing trade routes, and consequent further marginalization of smaller ports, which are many in the developing countries. This would not be neutral on the competitive position of traders from said countries.

Technology

An inconsiderate push towards a more extensive use of potentially costly technology, again, could affect the competitiveness of developing countries, should the lawmakers loose sight of the sustainability aspect.

Initially, good old basic common sense "pater familias" security measures and procedures in one's own backyard will often address the issue for individual exporters, importers or logistics operators' facilities, at least in the early stages. On this basis, more sophisticated sustainable technological enhancements can gradually be added that are proportionate to the size of the assets and the operations to be covered, as a result of a sound risk assessment.

To make a parallel, the ISPS Code does not mandate CCTV or biometrics, but does recommend fencing, access control, patrolling and appropriate lighting of the facility. Each entity must decide the most adequate technological enhancements it can afford, based upon its own specific cost/benefit analyses.

[2] US GAO report 08-538 on International Supply Chain security, August 2008

On the role of technology, the US Bureau of Customs & Border Protection (CBP) recently expressed that: "*DHS (department of Homeland Security) does not believe that, at the present time, the necessary technology exists to adequately improve container security without significantly disrupting the flow of commerce* "[3]

A great deal of work is still necessary to harmonize the various technologies derived from inventory control solutions, such as RFID, Infra Red seals, GPS-like tracking or similar, in order to ensure their mutual compatibility and interoperability through international standardization before they can even be considered as solutions worth being generalized to the container transportation. For example, the following areas need to be addressed: handling of alerts and tolerance levels, radio frequency allocation and standards, requirements for the installation and operation of the reading, transmission, communication and interface infrastructures. Many of the above issues will not have been solved in 2009, and there still exist concerns about the vulnerability of the devices themselves against "e-tampering".

A pragmatic note to conclude on technology: "*No one technology provides 100% compliance. A carefully selected mix to suit local conditions will become the norm*"[4]

Costs

A detailed study of the costs of SCS has yet to be made. Very preliminary estimates for scanning costs range from US$ 10 to US$ 440 per scanned container, depending of the throughput at the scanner. Active E-seals have been estimated to cost between US$ 10 and US$15 apiece. The estimated lifecycle cost for one of the new generation Advanced Spectroscopic Portal (ASP), a radiation detecting scanner developed under the aegis of the US Government, exceeds US$ 800,000, almost the triple of the cost of existing radiation scanners.[5]

Conclusion

There is no single path to achieve supply chain security. There is an overall consensus on the need to improve the security of the supply chains, world-wide. There is a multitude of programs, some endowed with the force of international law, others merely optional, with an array of in-between initiatives, including some that will likely become compulsory in practice, due to market pressure, and some others, technology-based, that are striving to become mandatory.

The layered approach seems to enjoy the broadest consensus, world-wide, and it is important to follow how it will fare in relation to the US 100% scanning law, and vice-versa. Within the layered approach, the mutual recognition between national certification programs remains a serious issue, in spite of a professed consensus.

Stakeholders also need to keep an eye on the question of technology. Some of the proposed technological solutions might provide significant improvements in the conduct of SCS measures. They must however adapt to the existing structure and infrastructure of international transport, and correspond and contribute to the needs and requirements of the transport industry and the international trade flows, not vice-versa. Technology-based solutions must remain proportionate, well thought-out, affordable and sustainable in all types of scenarios to reduce the risk of further marginalization of smaller ports and economies that could not afford the related investment and operational costs. In addition, lawmakers must ensure that endorsed

[3] Testimony of Acting Commissioner Jayson P. Ahern, U.S. Customs and Border Protection, before the House Appropriations Committee, Subcommittee on Homeland Security, on Cargo and Container Security, April 1, 2009
[4] K.Orchard, Generation Origin, May 2009 IAPH Conference
[5] US GAO report 09-655 "Combating Nuclear Smuggling", June 2009

technological solutions are mutually compatible and comply with universal technical and operational standards.

Finally, for Government Agencies, Port Authorities, private importers/exporters and transport operators, the time to start looking seriously at SCS is NOW.

1 INTRODUCTION

A *supply chain* is a system of resources, organizations, people, technologies, activities and information involved in the act of transporting goods from producer to consumer/user.

In the context of globalization, it also refers to the network of supply chains that form today's global commerce.

Threats to the supply chain can come:

- From outside the supply chain, threatening to disrupt the chain
- From inside the supply chain, when it is used to perform and cover illegal activities, like contraband, terrorism, or piracy.

Supply chain security (SCS) is the concept which encompasses the programs, systems, procedures, technologies and solutions applied to address threats to the supply chain and the consequent threats to the economic, social and physical well-being of citizens and organized society.

Unless explicitly computer related, the word program in this guide is understood as being a complex, a whole composed of interconnected or interwoven related parts, of integrated and sequenced methods, procedures, systems, rules and regulations applied to segments or components of the supply chain in order to enhance its security.

The programs that, in SCS parlance, are sometimes called "initiatives", may be:

- Global, regional, national, governmental, sectorial
- Multilateral, bilateral, unilateral
- Compulsory, voluntary.

They mostly apply to specific elements, areas, segments, sectors, links or events of the supply chain, or groups thereof. They may require the use of specific technologies or equipments, or sets thereof.

1.1 Background

This - (SCS) Guide is intended for Trade and Transport Government officials, Port Authorities and Transport, Cargo and Logistics Communities, in particular in developing countries. The guide will in broad terms describe all components of SCS and will preliminarily be directed toward Port and Trading Communities at large, but making references to other modes and nodal points as well.

This document is not an exhaustive encyclopedia of all the aspects of supply chain security.

Following the prevailing trend in the industry, the guide gives more attention to the maritime containerized transport than to other sectors or modes of transport, as it is currently the most evolutive sector.

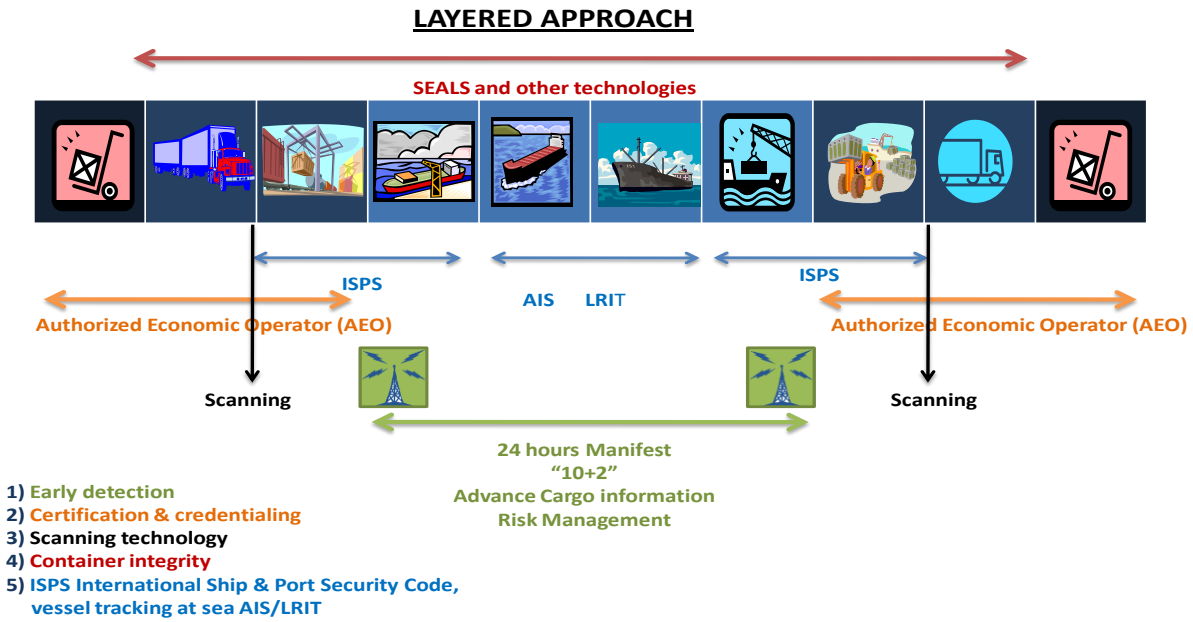
The purpose of the guide is to make concerned trade and transport-related officials, managers and personnel in developing countries acquainted with, and aware of, the many initiatives mushrooming in the field of supply chain security, what these will mean for their respective organizations, and how to tackle the inlaid challenges.

The main avenues presently explored in the pursuit of security in the supply chain are:

- The early detection of threats through the timely acquisition, analysis and validation of cargo information by the relevant Government Agencies, using advance cargo information broadcast and a consistent risk management system
- The certification or credentialing of the actors of the supply chain, to ensure that only legitimate, bona fide entities or individuals with an adequate security awareness and self-discipline actively participate to the supply chain. This ideally implies that mechanisms are in place for the mutual recognition by Governments of their respective certification programs
- The use of appropriate, sustainable technology to enable enforcement agencies to timely and speedily screen or examine a larger portion of the commercial flows, while facilitating the flows of legitimate trade.
- The improvement of cargo and container integrity during the whole transport cycle, centered on seals, track and trace, positioning and scanning technologies.
- A set of international regulations covering the tracking of vessels at sea, the interface between merchant vessels and ports and the security of the port facilities.

These five elements form what is being called a **multi-layered approach**. This approach is the one supported by the most active SCS drivers, namely the US Department of Homeland Security (DHS) and the World Customs Organization (WCO). The respective layers focus on different segments of the supply chain, providing multi-angle assessments of the cargo and ensuring that security does not rely on any single point that could be compromised. The idea is that the layers complement each other and reinforce the whole.

Figure 1-1 Layered Approach



1.2 Structure of the Guide

Considering the targeted audience, the guide will discuss the issues in the following sequence:

1.3 Supply Chain Security Programs

1. Major compulsory programs affecting the actors of the Supply Chain
2. Main voluntary programs (discussing those that are likely to become compulsory either by law or by market pressure)
3. Other significant programs.

1.4 Technology

1. Container integrity device technologies
2. Track & trace and positioning technologies
3. Non Intrusive Inspection technologies.

In addition, the guide offers a glossary, an index, a “linkography”, a FAQ section, elements for a roadmap for users in the form of specific checklists, and other annexes.

2 SUPPLY CHAIN SECURITY PROGRAMS

Multiple types of responses and actions have been undertaken by different governmental organizations, international organizations and businesses to enhance global SCS programs. These responses range from country-specific operational regulations to global research and pilot programs. All have different originating actors and target specific goals. These initiatives vary and they can be summed up by the following points:

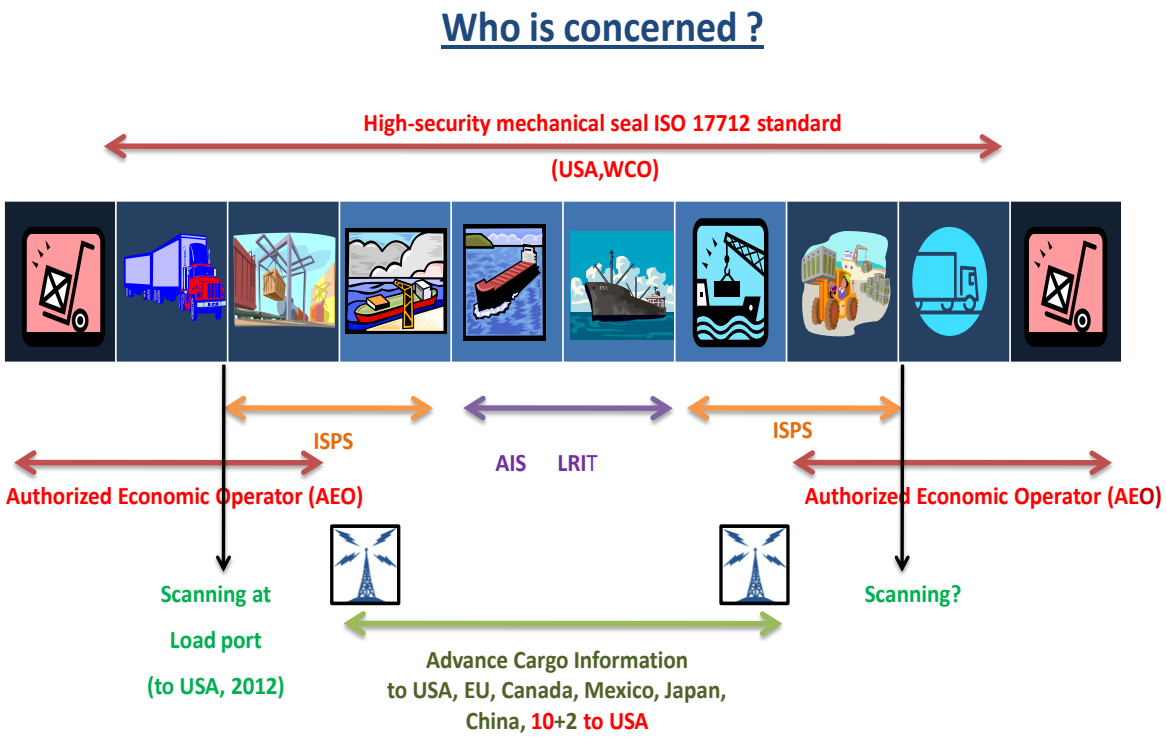
- **Type of originating actor**: International Organizations (IO's), Governmental agencies (i.e., Customs administrations, transportation authorities), private sector
- **Transport mode:** sea, air, road, inland waterway, and rail
- **Enforceability**: mandatory versus voluntary
- **Main specific goal**: enhancing Customs administrations security control capacity, reducing specific industry/geography vulnerability, developing global security standards, technology development / pilot projects.

(Gutierrez & Hintsa, 2006)

As outlined in the overview, the events of 9/11, and the resulting reaction from concerned governments, forced a new approach to supply chain initiatives, placing greater emphasis on security. More significantly, these events led to the establishment of new protocols for tracking and screening cargo both in the US and in other countries. These protocols have been incorporated into international frameworks seen for instance in those under the WCO, and in country-specific programs like the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI) administered by the US. Additionally, other countries, such as Canada, Australia and New Zealand introduced new cargo security programs post- 9/11 or strengthened previously existing programs. Many of these countries aim to harmonize their cargo security standards with those of the US and EU.

This chapter attempts to clarify the background and current status of the multitude of programs that exist across the world today. This is achieved by, firstly, giving a brief account of the changing security environment (post 9/11) and its resulting implications for SCS programs. This is important as it helps to explain the motivation of the programs which are later expanded upon in more detail within the chapter. Within this section, the motivations for different types of programs, not directly linked to the events of 9/11 but to other reasons, such as combating illegal activities, enhancement of efficiency and standardization are also explained. Secondly, a list of the main programs is presented under four main subheading- compulsory programs, major voluntary programs, regional/national programs and others. Tables are presented at the end of the section summarizing the main points of each program. Finally, some of the issues surrounding the programs are presented in the concluding section.

Figure 2-1 Who is Concerned



2.1 Evolution

The events of 9/11 precipitated a change in SCS measures. Prior to this event, the focus of governments was mainly on trade facilitation and harmonization of trade rules and practices as a result of the trade and customs environment imposed by the Kyoto Convention. After 9/11, global trade has experienced an extreme change in the existing paradigm from facilitation and harmonization to security and anti-terrorist measures. In the area of cargo security, prior to 9/11, Customs authorities were responsible primarily for clearing imported goods, after such goods arrived at the border. They did so through the review of entry documentation accompanying such goods at the time of importation and, if necessary, physical inspection of the goods.

In contrast, the cargo security programs developed after 9/11 emphasize pre-shipment controls applied to exports, illustrated in this chapter by the ACI programs enforced in the US, China, Japan, EU and Mexico. In particular, these programs require that exporters provide Customs documentation in advance of their shipment of goods to the importing country.

Such advanced information assists Customs authorities employing sophisticated and multilayered Risk Assessment techniques to determine whether to admit goods at the border or to hold them for further inspection and controls.

In addition, the focus of past private sector security practices was limited to "inside the company". This approach has now been broadened to encompass end-to-end supply chain security. Finally, due to the interconnection of threats in today's increasingly globalized world, coupled with the interdependencies of world trade, the previous country or geography-specific focus approach has been expanded to a global focus approach.

Many regional and international organizations have since reacted to the initial government-led changes - both in support of or against these changes. As it will be further demonstrated in the programs below, the role of these organizations has been mixed, ranging from attempting to standardize and coordinate these above-mentioned changes, or act as an independent mouthpiece advancing their own ideals and strategies.

The existing security programs have been created for different purposes and by different agencies or organizations. Four types of programs have been identified: i) Customs compliance programs to which a security layer has been added; ii) Government-originated pure security programs; iii) International Organization-originated security standards programs; and iv) Private sector pure security programs. Table 1 summarizes the main motivation and philosophy for each type of program and provides examples of programs belonging to each group.

Table 2-1 Identified types of SCS programs and their main aims

Type of Program	Examples	Main motivation and philosophy
Customs compliance programs to which the security layer has been added	PIP (Canada), ACP & Frontline (Australia), AEO (EU)	Customs administration aiming to streamline Customs processes (e.g. accounting, payment and clearance) for compliant importers/exporters. Due to new security concerns these programs have added a security layer. This implies that importers/exporters eligible for border crossing facilitation benefits should not only be Customs compliant but also low risk.
government origin, pure security programs	C-TPAT (US), Secured Export Partnership (New Zealand)	Governments and border agencies motivated by recent terrorist attacks. Security measures aiming to transfer some of the Customs control responsibilities to importers/exporters, in order improve the capacity to detect illegal activities. These programs have become prerequisites for participating in other Customs compliance programs.
IO's origin, security standards programs	WCO SAFE Framework of Standards, ISO (International organization for standardization), IMO (ISPS)	International Organizations aiming to establish SCS standards that can be generalized for the entire trading community.
Private origin, pure security programs	BASC (Latin America), TAPA (technology companies)	Private companies exposed to high risk of suffering from illegal activities in their cargo management operations. Security measures targeting the protection of cargo from being tampered or removed illegally

Source: Gutierez, X. and Hintsa, J., Voluntary Supply Chain Programs: A Systematic Comparison, 2006.

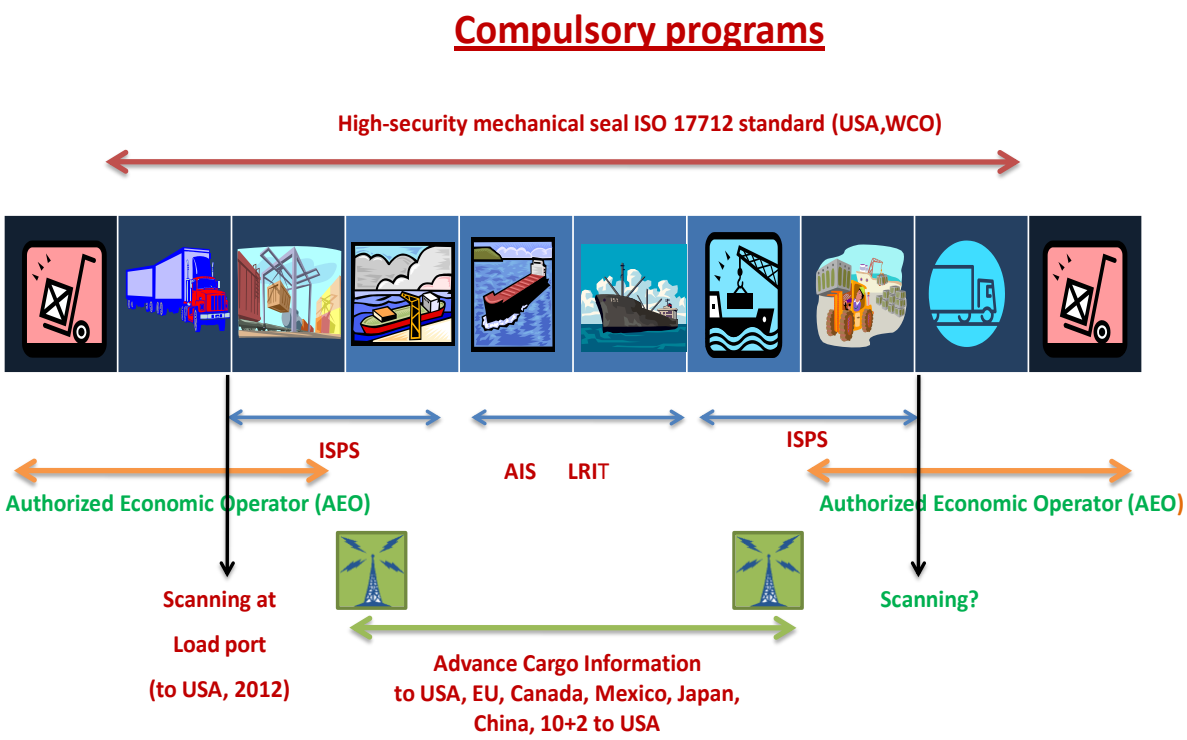
2.2 Compulsory SCS programs[6]

At the time of writing this guide, the following are the only nine compulsory SCS programs implemented internationally:

- The ACI 24 Hour Manifest Rule (US) (2003)
- The ISPS Code (2004)
- The ACI rules for the EU (2009-2011), Japan, Mexico (2007), Canada
- The ACI US 10+2 rule (2009-2010)
- The ACI rules in China (2009)
- 100% scanning (2012)

[6] In the list of compulsory programs might have been included AIS and LRIT (see glossary). These are remote vessel identification systems internationally enforced by the IMO SOLAS convention. They perform a tracking and tracing function at ship level (not at cargo level). They are discussed in parag. 2.6.8 & 9.

Figure 2-2 Compulsory Programs



1) Compulsory today
2) Compulsory soon

With the exception of the ISPS Code, 100 % scanning and ISO seal standards, the compulsory programs are all based on the Advance Cargo Information (ACI) concept and apply to trade moving to a given country or region.

The 100% scanning is mentioned here, because, while it is not materially in force today, it is nevertheless inscribed in the Security and Accountability For Every Port Act of 2006 (or SAFE Port Act[7]) as amended by the 9/11 Commission Act of 2007, namely a law in the USA (August 3, 2007 Public Law 110-53). Unless it is amended in the meantime, it will be enforced on the transport of maritime containers to the USA as from 2012.

The listed programs are defined as compulsory because one cannot move one gram of cargo to these countries if these rules are not implemented in one's supply chain.

2.2.1 Advance Cargo Information (ACI)

ACI is the concept that underpins the first compulsory SCS requirement, the 24 Hour Manifest Rule implemented by the US Customs in 2003. Additionally, US Customs & Border Protection (CBP) uses an Automated Targeting System (ATS) to support the ACI concept. ATS is in fact an Intranet-based enforcement and decision support tool that is the cornerstone for all CBP targeting and risk management efforts. CBP uses

[7] Not to be mixed with the WCO SAFE Framework of Standards (see para. 2.4.4)

ATS to improve the collection, use, analysis, filtering and dissemination of the massive quantity of ACI information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the US.

ACI is also an integral part of the World Customs Organization's SAFE Framework of Standards as one of the "four core elements". The WCO states that the "Framework harmonizes the advance electronic cargo information requirements on inbound, outbound and transit shipments". ACI is recognized in the US through the SAFE Ports Act which promotes the use of advance electronic information and origin-to-destination security.

The European Union (EU) has also incorporated the ACI concept within its Authorised Economic Operator (AEO) program. EU AEO requires the use of advance electronic data, electronic records, and security compliance to the EU Standards, adopts the Single Window concept, allows access to cargo and the control of seals on containers by authorized personnel only, and mandates control of cargo from loading to unloading.

This requirement, hitherto only compulsory for seaborne trade to the US, Japan, Mexico and China, is included in various programs across the world and is expected to be implemented by other countries, notably the EU, in the coming years. ACI provided by all the actors in the supply chain via the shipping lines allows Customs authorities to screen the imported containers, and make informed targeting and intervention decisions and to concentrate resources on the high risk issues and cargoes. This procedure, based on a Risk Management approach is considered one of the "cornerstones" in most SCS programs.

Some of the most relevant programs based on ACI are described hereunder, including the US 24 Hour Rule, the US 10+2 requirement, the EU Pre-arrival and Pre-departure Declarations, China 24 Hour Advanced Manifestation Rule, Mexico 24 Hour Rule and Japan ACI.

2.2.2 24 Hour Rule (US) (2003)

The 24 Hour Rule requires sea carriers and Non-Vessel Operating Common Carriers (NVOCCs) to provide US Customs and Border Protection with detailed descriptions of the contents of sea containers bound for the US 24 hours **before** a container is loaded aboard the vessel at the last foreign port. The Rule applies to all vessels which will call at a US port and all cargo destined for the US or carried via US ports to a non-US destination. The rule does not apply to feeder or transshipment vessels without a port call in the US. However, the Rule does apply when the cargo is transshipped onto a vessel with a port of call in the US.

In basic terms, the 24 hour manifest rule can be explained as follows: the shipping lines are not allowed to load a container onboard a vessel bound to a US port if they have not previously electronically communicated the basic bill of lading (manifest) details of the cargo contents, shipper and consignee of the container to US Customs 24 hours before loading. If the loading of a container is not expressly rejected by US Customs within 24 hours of the declaration, by default, it is allowed to be loaded to the US.

The required information includes the following:

- Shipper's name and address
- Consignee's or Owner's name and address
- Notify Address
- Bill of Lading Number
- Marks and Numbers from Bill of Lading
- Container Numbers and Characteristics

- Seal Numbers
- Cargo Description
- Gross Weight or Measurement
- Piece Count
- Hazmat Code
- First Foreign port/place carrier takes possession
- Foreign Port where cargo is laden abroad
- Foreign discharge/destination port for Immediate Exports and Transportation for Exports
- In-bond data.

In the case of non-compliance with the Rule, the most important consequence is denial of loading or unloading and a consequent disruption of cargo flows and supply chains. Furthermore, the US CBP may impose fines or other penalties on the carriers and others responsible for the submission of cargo declarations to US CBP. The rule allows US CBP officers to analyze the content information of the container and identify potential terrorist threats before the US-bound container is loaded at the foreign seaport, and not after it has entered a US port. The fact that the advance notification must be made 24 hours before a container is loaded means that when the vessel has arrived in the port of departure there is no more time available for advance notification of new shipments. Consequently, last minute shipments cannot be taken on board.[8] As far as air transport is concerned, the information shall be submitted to CBP directly after the departure of the flight. The most obvious impact of this rule deals with the timing of the manifest/pre-manifest data, i.e. the need to send shipment-related data to the regulatory bodies at an earlier stage. Further requirements include the more detailed description of the goods and data requirements to identify the various business partners within the supply chain.

Incidentally, it can be argued that the implementation of this Rule has produced improvements in the self-discipline of the players at the interface between the export shipping and maritime logistics industries. This in turn has induced significant efficiency gains in the port operations. In addition, potentially heavy fines, the risk to delay their vessels and the threat of a general deterioration of their relationship with the US CBP have convinced the shipping lines to willingly become the first line guardians of the scheme.

2.2.3 International Ship and Port Facility Security (ISPS) Code (2004)

The ISPS Code is an international agreement between government member states of the International Maritime Organization (IMO), which currently number 167. Being an international code, ISPS imposes itself upon the Governments of the signatory States. The ISPS Code addresses the security of the port installations and vessel components of the supply chain. The objective is to establish an international framework involving co-operation between signatory governments, government agencies, local administrations and the shipping and port industries to:

- Detect/assess security threats and take harmonized preventive measures against security incidents affecting ships or port facilities used in international trade
- Establish the respective roles and responsibilities of all the parties concerned, at the national and international level, for ensuring maritime security

[8] In not so ancient times, say 30 years ago, the rule for maritime documentation was that a "hard-copy" of the manifest (detailed recapitulative of all bills of ladings of cargoes loaded during a call) had to be remitted to the Captain of the vessel before the vessel sailed to the next port. A good Captain would never sail without his full set of manifests. The advent of Electronic Data Processing and internet allowed to significantly relax this rule, sometimes to the point of outright negligence.

- Ensure the early and efficient collaboration and exchange of security-related information
- Provide a methodology for security assessments so as to implement plans and procedures to react to changing security levels; and
- Ensure confidence that adequate and proportionate maritime security measures are in place, both ashore and on board merchant vessels.

The ISPS Code applies to all cargo ships of 500 Gross Tons (GT) or above, passenger vessels, mobile offshore drilling units and port facilities serving such ships engaged on international voyages. The security requirements generally call for ships and port facilities to conduct security assessments, develop and implement security plans, and appoint security officers and security personnel. The security assessments must identify the vulnerabilities of assets and infrastructure to a security incident. The security plan must specify the measures that will be implemented at three escalating security levels representing the prevailing threat environment to address the identified vulnerabilities. At a minimum, the plan must address access control, security monitoring, restricted areas, cargo, stores and unaccompanied baggage, drills and exercises, and security duties and training. Company, ship, and port facility security officers must also be designated as the individuals responsible for ensuring implementation of the respective security plans. The application of the security measures outlined in the ISPS code lends confidence that ships and ports complying with ISPS maintain a certain standard of security, based on internationally prescribed criteria.

ISPS establishes a mandatory permanent and structured dialogue between ports and vessels, which have to mutually declare/confirm their respective level of security. When one registers a security breach, the other has to correspondingly raise its own alertness level and procedures, generally by intensifying basic security measures like: access control, searching of vehicles, increased patrolling.

While many ports and vessels were already ISPS-compliant even before the code was implemented, ISPS has had the merit to drastically improve the security level of laid-back port authorities and substandard vessels, by focusing on basic discipline and solid “common sense” physical security measures, such as: access control, lighting, fencing and proactive patrolling.

Once installed and running, the network auto-regulates itself. Recurrently non-compliant vessels will be subject to more and more controls, and will gradually experience difficulties to find ports that will welcome and operate them. Vessel operators will become more and more reluctant to call at repeatedly non-compliant ports, as non-compliant ports or vessels mutually taint each other. Eventually, serial offenders will find themselves ostracized by the market itself, if they are not arrested or boycotted before. That being said, although it has the strength of an internationally ratified code, ISPS has had its share of teething problems, and, even today, it can be said that it is not applied with the same zeal in all the ports. Lessons can be drawn from this for the implementation of compulsory SCS programs.[9]

2.2.4 Pre-arrival and Pre-departure (EU*)* (2009-2011)

This program is the EU version of ACI. The program proposed by the European Commission began in 2005, will be implemented in July 2009 and will come into full effect in 2011. It has been designed to meet the need for safety and security in relation to goods crossing international borders, including requirements linked to the US CSI, while, at the same time, remaining in step with the EU e-Customs plans for the future. Its intention is to

[9] For more information on ISPS refer to the IMO’s FAQ on ISPS Code and maritime security. http://www.imo.org/Newsroom/mainframe.asp?topic_id=897_and Review of Cost of Compliance with the New International Freight Transport Security Requirements. http://siteresources.worldbank.org/INTTRANSPORT/Resources/tp_16_ISPS.pdf

provide Customs authorities with advance information on goods brought into, or exported from the Customs territory of the European Community. This is intended to provide for better risk analysis, but, at the same time, for quicker process and release upon arrival, resulting in a benefit for traders that should be equal to, if not exceeding, any cost or disadvantage of providing information earlier than at present.[10]

The European Union has put into place transitional arrangements for the implementation of the ACI requirement:

Shippers will not be required to submit Pre-Arrival declarations and pure Exit Summary declarations in electronic format until January 1, 2011, under transitional arrangements agreed by the EU, except for export declarations which require safety and security data as from July 1, 2009.

This means that shippers using the Import Control System (ICS) and the Export Control System (ECS) and who are prepared to make entry and exit summary declarations, may voluntarily do so starting on July 1, 2009, but they are not as yet obliged. Shippers who are prepared, but operating in member states that are not ready yet, will not be able to do so. This delay does not, according to the European Commission, relieve customs administrations from the obligation to continue implementing the systems allowing for electronic submission of exit/entry summary declarations as soon as possible.

2.2.5 Japan ACI (2007)

Implemented by the Japanese government in 2007, this ACI program is applicable to sea and air cargo arriving in Japan. For ocean-going vessels it requires that the following cargo information: place of shipment, place of destination, marks & numbers, cargo descriptions, quantities, shippers and consignees of goods, bill of lading number and container number is made available at least 12 hours, but no longer than 24 hours, before the arrival of the vessel at the port of destination in Japan.

Similarly, air cargo information is required at least three hours, but no longer than five hours before cargo arrives at the airport in Japan from overseas. Failure to comply, such as not filing information by the specified deadline or providing false information, is subject to the following penalties: a) for a vessel or aircraft which moves/flies between a foreign country and Japan for foreign trade 500,000JPY or less; b) for a vessel/aircraft other than above 300,000JPY or less.[11]

The following section describes the major programs in which ACI requirements are used, such as the development of a single window for importers and exporters, the unique consignment reference and various Customs data models.

2.3 Mexico 24-hour Rule (2007)

The Mexico 24-hour Rule, similar to the security regimes developed in other countries, requires all transporters of maritime cargo to Mexico to electronically submit cargo manifests to the Mexican Customs 24 hours prior to loading Mexico-bound shipments at foreign ports of loading. Oceans carriers, freight forwarders and NVOCCs who issue bills of lading to transport cargo to Mexico must file through Mexico Customs for their

[10] This information is based entirely on the European Commission's Commission Directorate Gerneral on Taxation and Customs Union: "Pre-arrival/Pre-departure"
http://ec.europa.eu/taxation_Customs/customsCustoms/procedural_aspects/general/prearrival_predeparture/index_en.htm

[11] The information is based from information from documents gained from Japan's Customs. For further information please visit their website http://www.customs.go.jp/english/procedures/advance_e/index_e.htm

shipments, with the exception that ocean carriers cannot file on behalf of their freight forwarder/NVOCC customers.

2.3.1 10 + 2 (2009-2010)

In January 2009, the US CBP introduced a new program, called the Importer Security Filing (ISF) or more commonly called 10+2, which requires cargo information for security purposes to be transmitted to CBP at least 24 hours before goods are loaded on a vessel for shipment to the US. This new rule is pursuant to section 203 of the SAFE Ports Act, and requires importers to provide 10 data elements to the CBP with the carrier providing 2 additional data elements.

This program originates from the realization that CBP cannot derive the optimal, most efficient cargo risk assessments based only on ocean-carrier bill of lading data. Those familiar with maritime transport documentation will recognize that the cargo description and shipment information mentioned on a maritime bill of lading is, in the case of full containers, solely a shippers declaration, which, by nature, the ocean carrier has no means to verify. Hence the "container said to contain" and "shippers' load, stow and count" clauses on the bill of lading. 10+2 is meant to provide another set of data directly from the importer for screening by CBP's targeting and risk management tools.

As mentioned above, the new rule came into effect on January 26, 2009. CBP is taking a phased approach in terms of implementation and enforcement. During the first 12 months, importers will be warned of infractions instead of being fined. After this 12 month grace period," (that is, as from January 1st 2010), importers can face fines up to US $5,000 for each violation.

The following are the ten data elements that must be transmitted to CBP as part of the ISF Importer Security Filing (ISF):[12]

- Manufacturer's name and address
- Seller's name and address
- Consolidator's name and address
- Container stuffing location (Address at which goods loaded into a container)
- Buyer's name and address (Last named buyer)
- Ship to name and address (Party physically receiving the goods)
- Importer of record's number
- Consignee's number
- Country of origin
- Harmonized tariff schedule number (to the 6th digit).

CBP also requires two additional elements to be provided by the ocean carrier at least 48 hours after departure from the last foreign port, or prior to arrival for voyages less than 48 hours in duration:

- Vessel stowage plan
- Container status message.

This will enable CBP to detect erratic or abnormal behavior by a given container during sea-passage.

[12] For a detailed description of each item, please consult : http://www.cbp.gov/

2.3.2 China 24-hour Advance Manifest Rule (2009)

Starting on 1 January 2009, this Rule, implemented by the Chinese government, requires ocean carriers to submit the manifest or the bill of lading (similar to those of other programs mentioned above) to the Chinese Customs 24 hours prior to loading of the cargo. This rule is applicable to all export, import, and transshipped cargo via any Chinese ports.[13]

2.3.3 100% scanning (2012)

A bill was passed in the US in 2007 under the title "Implementing Recommendations of the United States 9/11 Commission Act of 2007" mandating overseas radiation scanning and NII inspection of 100% of all cargo containers destined for the U.S. by 2012. Regulated by the US CBP, this program is seen as a major effort to enhance national security by preventing weapons of mass destruction (WMD) from entering the US, but in a way that does not compromise the economic vitality of the country and ensures trade facilitation.

To fulfill these requirements, the SAFE Port Act mandated a pilot project phase in three ports to assess the feasibility of scanning 100 % of shipments coming to the United States. These ports included: Qasim, Pakistan; Cortes, Honduras; Southampton, UK. At these ports, 100 % of the cargo exported to the US is scanned for radiation, and an image of the contents is taken, using large scale non-intrusive imaging equipment. The radiation alerts and scan images are analyzed either on the ground by CBP personnel, or back at the CBP National Targeting Center (see also the section on SFI).

There has been much debate surrounding the ability, practicality and effectiveness of implementing this law by 2012.

Many trade partners of the US, more specifically the EU, consider this legal obligation as unilateral and implying extraterritoriality. According to many analysts, it will work at cross purposes with the layered approach hitherto generally adopted, and could even undermine the current overall SCS initiatives by instilling a false sense of security. The technologies needed to implement 100 % scanning are hardly available at an operational level. Among others, while radiation detecting equipment generates automatic alarms, NII imagery still needs human review and analysis. On such a scale as imposed by the bill (100% scanning) there are concerns that the massive need for skilled manpower will end up diverting scant human resources from more specialized non-repetitive tasks.

While investment and operational costs are predicted to be on the very high side, it is also argued that one impact of the legislation will be an artificial transformation of the traffic flows and patterns in favor of the bigger ports, to the prejudice of the smaller ones.

To illustrate the deep puzzlement experienced by the Trade Community in general, and the port and maritime transport industry in particular, the below extract from the Testimony of Acting Commissioner Jayson P. Ahern, U.S. Customs and Border Protection, before the House Appropriations Committee, Subcommittee on Homeland Security, on Cargo and Container Security on April 1, 2009 speaks for itself :

"Scanning all 11.3 million containers that enter (yearly) U.S. seaports from a foreign port presents significant operational, technical, and diplomatic challenges. They include:

[13] Further information on the exact rules can be found For further information on these rules please visit the following website http://www.iata.org/NR/rdonlyres/41C5E2B2-9A4D-4D9B-A010-EFBF5304174F/0/PRCCustomsPolicyNo172.pdf

- *Sustainability of the scanning equipment in extreme weather conditions and certain port environments*
- *Varying and significant costs of transferring the data back to the United States (National Targeting Center) in real-time*
- *Re-configuring port layouts to accommodate the equipment without affecting port efficiency and getting the permission of host governments*
- *Developing local response protocols for adjudicating alarms*
- *Addressing health and safety concerns of host governments and local trucking and labor unions*
- *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*
- *Concluding agreements with partnering nations and terminal operators to document roles and responsibilities regarding issues such as ownership, operation, and maintenance of the equipment; sharing of information; and import duty and tax considerations*
- *Staffing implications for both the foreign customs service and terminal operator*
- *Licensing requirements for the scanning technology*
- *Host government support for continuing to scan 100 % of U.S. bound containers after the pilot ends; and the potential requirements for reciprocal scanning of U.S. exports."*

100% scanning costs estimates

Analyzing the results of the "live" tests conducted in Southampton in the frame of the SFI program, the European Commission, Directorate General Taxation and Customs Union commented to CBP in April 2008:

"For relatively small ports, the introduction of 100% scanning would require very high investments and important human resources devoted to it. In the case of Southampton, a simple calculation of total cost relative to the number of scanned US bound containers gives an average cost/container that exceeds US$ 500."

Another attempt to evaluate the related costs was made in June 2008 by the University of Le Havre, sponsored by WCO, gave a range of US$ 10 to US$ 440 per scanned container based on volumes ranging from 420,000 to 5,000 containers scanned per year.[14]

Port operations in Asia are predicted to suffer the largest impact of the new law, since over 50% of US imports are loaded in China. John Lu, Chairman of the Asian Shipper's Council commented that the legislation will "*slow down cargo and cause a gridlock at ports*", echoed in this from Singapore:

"There is also the danger that unilateral measures on maritime and cargo security, such as the recent requirement that all US-bound containers be scanned in foreign ports by 2012, will slow down the flow of trade. A balance must be struck between ensuring security and facilitating trade, if we are to preserve the efficiency of shipping and cargo operations and allow global trade to flourish. (…)

Asia will have to safeguard its maritime interests, and ensure that they are accommodated in the on-going Western-driven development of a global framework of rules and standards governing international shipping (…). We can expect more Asian voices to enrich the deliberations at international forums to tackle issues that cannot be solved unilaterally or regionally. (…) To ensure that the measures introduced are sensible and pragmatic, a multilateral approach is more likely to produce sensible and pragmatic solutions than uncoordinated unilateral initiative."[15]

There is, however, currently no study establishing clearly the expected major cost impact that 100% scanning would have by inducing a decrease in the efficiency of port operations as an effect of physically slowing down and disorganizing transport flows in the terminals.

Critics of the legislation also contend that the technology to scan the yearly 11 million US-bound containers at foreign ports is currently not sufficient to satisfy the requirements. Moreover, Làszlo Kovàcs, the European Commission's Taxation and Customs Union Commissioner, states that if implemented, this measure would cause serious disruption and an additional administrative burden in more than 600 ports worldwide for cargo that leaves for the US. These ports had been already straining to cope with increasing trade volumes (WCO News, 2008).

An article in the Wall Street Journal by John Miller (2007) highlighted several port concerns. Analysts believed that each port would have to buy 1 to 10 scanners to comply with the new legislation. The EU estimated the average initialization cost of a port to be around US$100 million, a cost too large to be justifiable for some of

[14] Global Logistic Chain security, Economic impact of the US 100% scanning law, University of Le Havre/WCO June 2008
[15] Opening address my Mr. Lee Kuan Yew, Minister Mentor, at the inaugural Singapore Maritime Lecture, 25 September 2007

the smaller ports with very few US-bound containers. Even if ports are financially capable of purchasing the scanning equipment, they are faced with other problems such as space constraints.

Miller believes that the 2007 9/11 Act might even change the dynamics of port competition. Larger ports might strive to gain new business from smaller and from older ports that are financially strained to meet the requirements of 100% scanning. The EU has expressed concerns that Asian ports, being newer and more compact, would have an advantage in meeting the requirements. Smaller ports might have to stop shipping to the US altogether if they are unable to bear the financial costs of installation. "*The law will force us to stop shipping to the US, unless we can attract a lot more customers, which would justify investment in the equipment*," said Philippe Revel, Manager at Dunkirk, France (Miller, 2007,). The EU has also threatened to impose reciprocity and require the US to scan all European-bound containers if the 100% scanning legislation is not altered.

The 2012 deadline

In February 2009, Secretary Napolitano of the US Department of Homeland Security (DHS), alerted the US Congress that due to logistical concerns expressed by shippers and carriers and diplomatic concerns expressed by foreign governments, it was envisaged that DHS will not meet the 2012 deadline to scan all cargo bound for US seaports.

The law already contains provisions for a grace period of 2 years, if a number of conditions cannot be met. However, beware, the 9/11 Act also allows an implementation earlier than 2012 – which could occur if a significant security incident should happen to involve containers. [16]

[16] K.Orchard, Generation Origin, May 2009 IAPH Conference

Table 2-2 Summary of main compulsory programs

Name/ Year implemented	Originated Country/ Institute	Regul. Body	Route Covered	Modes	Participation /Status	Category	Goal
24 Hour Rule (US), (2003)	US	Customs	From any Country to US Import	Sea	US ports	Govt.- Mandatory	Advanced information
ISPS, (2004)	IMO	IMO	World-wide	Ships and Ports	167 member states	International/ mandatory	Stand. & consist. framework for evaluating risk
Pre-arrival & Pre-departure EU(2009-11)	EC	Member state Customs	Within EU,and any country to EU	Sea	All EU member states	EU-will become Mandatory on 1-1-2011	Advanced information
Japan ACI, (2007)	Japan	Customs	From any country to Japan(imp.)	Sea and air	Japan ports and airports	Govt.- mandatory	Advanced information
Mexico 24 hour Rule (2007)	Mexico	Customs	From any country to Mexico (Import)	Sea	Mexico ports	Govt.- mandatory	Advanced information
10+2 (2009) US	US	CBP	From any country to US (Import)	All	US ports	Govt. mandatory	Advanced information
China24hour Advanced Manifestation Rule, (2009)	China	Customs	From any country to China (Import)	Sea	China ports, except for Hong Kong and Macau	Govt.- mandatory	Advanced Information
100 % scanning, (2012)	US	CBS	Global (to US)	Ships & Ports	Pilot phase, 5 ports operating	International mandatory in 2012	Comprehensive SCS

2.4 Major Voluntary programs

These programs are labeled voluntary because they are not compulsory, in the sense that they are not imposed by a law or international code or convention. In theory, trade and transport operators can still operate – albeit possibly at a competitive disadvantage – without participating to one of these programs.

2.4.1 Transported Asset Protection Association (TAPA) (1997)

TAPA is a pre- 9/11 program. It is a non for profit association which was formed in the US in 1997 and which started working in Europe in 1999 and in Asia in 2000. TAPA's rationale for coming into existence was motivated by an observed rise in cross-border crime in the United States. According to TAPA, the introduction of the EU's inner market during this period, made it easier for criminal gangs to move across borders. TAPA EMEA (TAPA Europe, Middle East and Africa) considers this to have had a major impact on crime directed towards the transport of goods with a high value.

TAPA's overall goal is to identify the fields in which members experience losses, and to share information on effective routines and practices. The program concentrates its efforts on the transport of high-tech goods; the possibility to become a member of the program is limited for an average sized company. Initially, only companies that produce or export high tech goods could become members, but this was later extended to include companies producing other high value goods.

Due to this TAPA has an exclusive image, and mainly high-profile companies are involved. TAPA's security measures focus on truck transportation and do not extend to container transport at sea.

Since TAPA began it has established two main initiatives: the Incident Information Service (IIS) and the Freight Suppliers Minimum Security Requirements (FSR). IIS is a service for the exchange of security-related information that TAPA provides for its members. FSR are requirements that are placed on general security in the supply chain and which include, among other things, external security, premises and security routines.[17]

2.4.2 Customs-Trade Partnership Against Terrorism (C-TPAT*)* (2001)

The C-TPAT program is a joint effort between the US government and businesses involved in importing goods into the US. It is part of the ever-evolving nature of the US CBP post 9/11, and recognizes that border security will be much more efficient if Customs involves businesses in the process of securing and inspecting cargo. The approach, which began in 2001 with 7 large US companies, was geared towards acting against possible supply chain terrorism, especially to do with container security. Since then C-TPAT has grown markedly to the extent that over 8,000 companies are now actively involved with the C-TPAT process. CPB Agents have participated in over 4,000 validation reviews and have met with C-TPAT Partners in over 50 countries.

Currently, the C-TPAT covered route encompasses any country importing into the US and is applicable to all transport modes.

Membership in C-TPAT is available to most businesses that import goods into the US including freight carriers, brokers, manufacturers, and importers, as long as they agree to the guidelines of C-TPAT membership. In addition to supporting the US global war on terrorism, C-TPAT membership also carries a number of tangible benefits. Members are less subject to Customs inspections, and C-TPAT containers that are singled out for inspection go straight to the front of the line, ahead of non-C-TPAT boxes.

A rough estimation of "green lane" benefits of AEO-programs membership is proposed by CBP : "*C-TPAT membership often results in reduced security inspections;* ***C-TPAT importers are 6 times less likely to incur a security examination and 4 times less likely to incur a compliance examination "***[18]

The C-TPAT member has to verify that its own partners, subcontractors, suppliers, address the required security elements and it is only the C-TPAT member that derives the benefit and not the partners, unless they are also C-TPAT members. The C-TPAT members can also take advantage of C-TPAT training for their employees, to learn about more ways to strengthen the security of their supply chain. If routine inspection shows non-compliance, C-TPAT membership is withdrawn and the company must re-certify.

C-TPAT membership is voluntary for any business, though most large companies have joined due to the perceived advantages it offers. Additionally, a company does not have to be American to join C-TPAT. CBP's strategy relies on a layered security approach consisting of the following five goals:

1. Ensure that C-TPAT partners improve the security of their supply chains pursuant to C-TPAT security criteria.
2. Provide incentives and benefits to include expedited processing of C-TPAT shipments to C-TPAT partners.

[17] This section is based primarily from information gathered from TAPA website. For more information see http://www.tapaemea.com
[18] Testimony of Acting Commissioner Jayson P. Ahern, U.S. Customs and Border Protection, before the House Appropriations Committee, Subcommittee on Homeland Security, on Cargo and Container Security 1 April 2009

3. Internationalize the core principles of C-TPAT through cooperation and coordination with the international community.
4. Support other CBP security and facilitation initiatives.
5. Improve administration of the C-TPAT program.

Special requirements of C-TPAT membership entail that members must agree to leverage their service providers and business partners to increase their security practices. In fact, many companies are demanding that their business partners enroll in C-TPAT or adhere to its security guidelines, and they are conditioning their business relationships on these requirements. If a business partner has been certified and validated in C-TPAT, there is no need to obtain further information from that partner in terms of their compliance with C-TPAT security criteria or guidelines.[19]

2.4.3 Container Security Initiative (CSI) (2002)

CSI was established in 2002 by the US CBP to address the threat to border security and global trade posed by the potential terrorist use of a maritime container. Participating countries establish a security regime in cooperation with the US CBP to ensure all containers that pose a high risk for terrorism are identified and inspected before they are placed on vessels destined for the US. Moreover, CSI aims to target and pre-screen containers and to develop additional investigative leads related to the terrorist threat to US-bound cargo. As the CBP puts it, the intent is to "extend [the] zone of security outward so that American borders are the last line of defense, not the first". Prior to the establishment of CSI, there was no foreign inspection of US-destined containerized shipments. The security of maritime containers pre 9/11 was limited to targeting and inspection upon arrival in the US, an approach deemed to be burdened with significantly greater risk. The US Department of Homeland Security (DHS) considers that this security regime, designed for the maritime container environment, greatly enhances and complements the Layered Security methodology being employed by CBP in C-TPAT.

In the CSI program high-risk shipments are identified and examined by using cargo security measures, such as X-ray and radiation scans. For example, high security Mechanical Seals and Tamper Evident Tape are applied after the examination of containers in order to maintain the integrity of the container while in-transit to the US. Currently, there are 58 operational CSI ports in Europe, Asia, Africa, the Middle East, and North and South America. This translates to 86% of all maritime containerized cargo destined to the US being covered. A further 35 Customs administrations have committed to join CSI.[20]

The voluntary CSI program aims to foster a collaborative working relationship with the participating foreign governments, promoting, among other things, the sharing of intelligence, local trends, and best practices. The program is envisioned to play a vital role during periods of increased risk, heightened threat levels, and in re-establishing the flow of commerce in the event of a security incident. The CBP Commissioner has requested all of the director generals of CSI partner countries' Customs administrations to heighten screening and examination of cargo shipments during periods of increased risk.

[19] This section information is based primarily on the US Customs and Border Protection document "Securing the Global Supply Chain, Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan.
http://www.housewares.org/pdf/iha/global/CTPATStrategicPlan.pdf

[20] These figures are according to a 03/27/2008 report titled Container Security Initiative, and are available at
http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade_security/csi.xml.

The countries that want their ports to be CSI ports must fulfill a large number of special requirements. Their Customs administration must be technically capable of implementing Non-Intrusive Inspection[21] (NII) of all goods that are imported, exported, in transit, or transshipped through the country. The port in question must have direct, regular and substantial container traffic to ports in the US. The port authorities, together with the Customs, must undertake to produce a risk management program that can identify possible high risk containers. Furthermore, the country's authorities must be prepared to share information with the US and CBP to facilitate a joint focus on high risk objects, and be prepared to introduce an automated mechanism for this exchange of information.

2.4.4 World Customs Organization SAFE Framework of Standards (2005)

At the June 2005 annual Council Session in Brussels, the WCO Members unanimously adopted the "*SAFE Framework of Standards to secure and facilitate global trade*".

The Framework aims to:

- Establish standards that provide supply chain security and facilitation at a global level to promote certainty and predictability.
- Enable integrated supply chain management for all modes of transport
- Enhance the role, functions and capabilities of Customs to meet the challenges and opportunities of the 21st Century
- Strengthen co-operation between Customs administrations to improve their capability to detect high-risk consignments
- Strengthen Customs/business co-operation
- Promote the seamless movement of goods through secure international trade supply chains.

The SAFE Framework consists of 4 core elements:

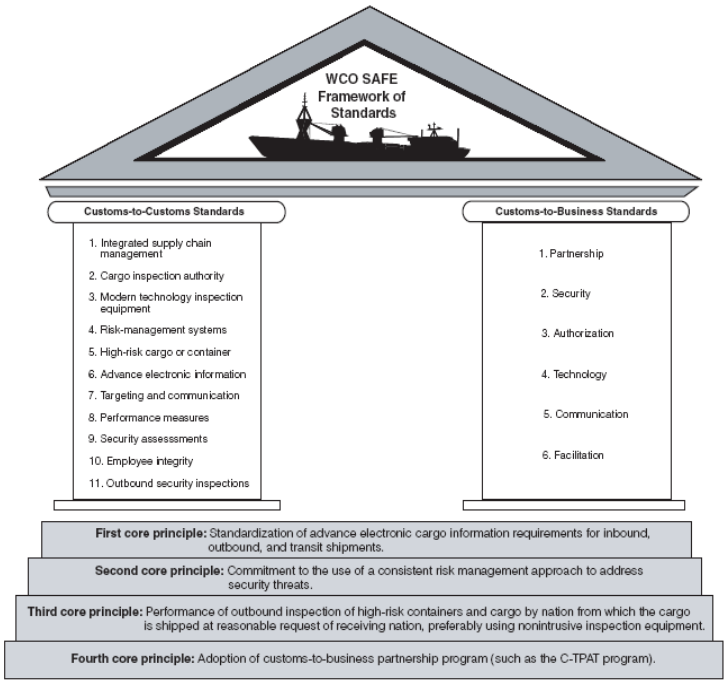
- The Framework harmonizes the ACI requirements on inbound, outbound and transit shipments
- Each country that joins the Framework commits to employing a consistent risk management approach to address security threats
- The Framework requires that at the reasonable request of the receiving nation, based upon a comparable risk targeting methodology, the sending nation's Customs administration will perform an outbound inspection of high-risk containers and cargo, preferably using non-intrusive detection equipment such as large-scale X-ray machines and radiation detectors
- The Framework defines benefits that Customs will provide to businesses that meet minimal supply chain security standards and best practices.[22]

The Framework, based on the previously described four core elements, rests on the Twin Pillars of Customs-to-Customs network arrangements and Customs-to-Business partnerships (see figure 1.1). The pillars involve a set of standards that are consolidated to guarantee ease of understanding and rapid international implementation.

[21] These are inspections that are made without having to enter a container physically, which is often costly and can create delays in the flow

[22] This section information is based primarily on World Customs Organization's SAFE Framework of Standards, document, available at http://www.wcoomd.org

Figure 2-3 The Twin Pillars of the WCO SAFE Framework of Standards



Source: U.S.Government Accountability Office, Report GAO-08-538.

The WCO has taken the lead to develop the SAFE Framework. In essence, the WCO SAFE Framework provides a blueprint for implementing a national, regional and international SCS approach. Since the adoption of the SAFE FoS, work has progressed on improving the program, principally by incorporating into its text detailed provisions concerning AEO which had been initially developed in a separate document.

To date, out of 174 WCO Members, 156 have signed the letter of intent to implement the SAFE FoS, representing approximately 95 % of global international trade. In addition, 110 WCO member Customs administrations have requested capacity building assistance from the WCO through the Columbus Program (for further information on this program see 1.5.5). So far, over 107 WCO Members have received a needs assessment mission and a diagnostic report summarizing the findings of the mission and providing a series of recommendations. Over 60 administrations have entered the implementation phase. [23] At Council sessions WCO Members are provided with a "Global Trends and Patterns Report" that presents information on implementation activities and achievements, and with "Regional Trends and Patterns Reports" which presents findings from the diagnostic missions.

It is however reported that – not unexpectedly, considering the scope of the task at hand – the implementation of the SAFE Framework is suffering from similar teething problems as experienced during the implementation phase of the ISPS Code. The level of awareness and preparedness is extremely variable from one country to another. The progress in the implementation of the SAFE Framework directives, therefore, remains largely uneven, which has prompted the WCO to multiply its efforts towards capacity building and large scale training (see Columbus Program). In the meantime, businesses are often left with serious doubts about their own way forward, and the costs thereof.

[23] For the latest information on the exact status of this program visit the WCO website: http://www.wcoomd.org

It has been debated whether the WCO SAFE Framework of Standards should be categorized as a voluntary or a compulsory program. On one hand, it is often presented as a platform and calls itself a framework. Its initial version counted only 40 pages and the WCO Members have only signed "letters of intent" to implement it and no enforcement deadline has been set. On the other hand, considering the power of the WCO as prime mover, one can be certain that it will shape the vast majority of the future AEO certification programs (which, incidentally, is boding well for the mutual recognition and interoperability dimension within SCS as a whole).

2.4.5 ISO 28000 series (2005)

ISO/PAS 28000:2007, Specification for Security Management systems for the supply chain (commonly referred to as the ISO28000) is the ISO series of standards addressing security in the supply chain. The standards are regulated by ISO and can be applied internationally to all routes and transport modes. The idea behind this standard is to facilitate better controls of flows of transport, to combat smuggling, to meet the threats of piracy and terrorism, and to create a secure management approach to the international supply chain.[24] ISO 28000 is a security standard based upon the so-called Plan-Do-Check-Act method which the ISO explains in the following way:

- **Plan**: to specify necessary goals and procedures to achieve results, in line with the organization's security policy
- **Do**: to introduce the routines in question
- **Check**: to check and measure procedures on the basis of the security policy, goals and objectives
- **Act**: to continuously improve security management systems.

The system proposed in ISO 28000 includes aspects such as financing, production, information management and packing, storing and transport of goods. It shall be possible to implement by organizations of all sizes, from small-scale to multinational, that wish to:

- Establish, implement, maintain and improve a security management system;
- Assure compliance with stated security management policy;
- Demonstrate such compliance to others;
- Seek certification/registration of its security management system by an accredited third party certification body; or
- Make a self-determination and self-declaration on compliance with ISO 28000.

In particular, ISO28001 offers down-to-earth best-practice data for local SCS implementation.

The management of an organization shall draft and adopt a comprehensive security policy. This policy shall be adapted to ensure that it corresponds with the organization's other policies. It shall also be adapted to identify threats against the organization. The policy shall be documented and published and all members of the organization shall be informed about it. The organization can choose to have a detailed security policy for internal use which can be confidential and a brief and a non-confidential version, which parties, outside the organization, can be given access.

It is expected that ISO 28000 series will facilitate trade and the transport of goods across borders. It will also increase the ability of organizations in the supply chain to effectively implement mechanisms that address

[24] For example, Dubai Port World (DPW), 4th biggest global terminal operator already has 22 ISO28000-certified sites and expects to have its full terminal portfolio compliant by 2001. All its new terminals are designed for ISO 28000 certification.

security vulnerabilities at strategic and operational levels, and to establish preventive action plans. Organizations can then continually assess their security measures to protect their business interests, and ensure compliance with international regulatory requirements.

By encouraging the implementation of these standards by the various actors in the supply chains, countries will be able to maximize the use of government resources, while maintaining a level of optimal security.

The ISO 28000 series is indeed a complementary approach to governmental, international and Customs agency security initiatives, including the WCO's SAFE FoS, the EU's AEO, the US's C-TPAT and the IMO's ISPS.[25]

2.4.6 EU Authorized Economic Operator (AEO) (2008)

As defined by the WCO, an AEO is "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." This definition comes from the WCO SAFE Framework where there is a tenet to create a set of international standards with respect to SCS to promote uniformity and predictability across Customs organizations. The EU AEO program is a plan devised by the European Commission with the goal to provide reliable traders with trade facilitation measures. The program is mandatory for EU member countries and voluntary for companies.

While not a mandatory program for companies, there are thought to be numerous benefits through becoming AEO certified, such as, expedited cargo releases, reduced transit times, access to special measures during times of trade disruptions or elevated threat levels, and priority during cargo checks. All companies looking to become AEO certified will need to engage in a self-assessment of their global supply chains using a pre-determined set of security standards and best practices. In this assessment suppliers will need to demonstrate an adherence to policies and procedures that safeguard against any loss of integrity of their shipments until released from Customs control at destination.

The self-assessment process must include the following:

- Pre-determined security best practices are incorporated into existing business practices
- Validation process has been completed by a recognized Customs agency
- Modern technology is utilized to maintain all shipments (including the container) integrity
- Open communication with Customs authorities to receive minimum security standards updates and SCS best practices.

Table 2-3 Identified types of SCS programs and their main aims

Name/. Year started	Originated Country/ Institute	Regul. Body	Covered route	Mode	Participation/ Status	Category	Goal
TAPA, 1997	US	BoD	Only truck transport routes in US, ME, AF, and Asia	Truck	207 members	Private voluntary	Crime incident reporting/ identify solutions/share information

[25] For more information see the ISO's ISO28000 Specification for Security Management Systems for the Supply Chain: http://www.iso.org/iso/catalogue_detail?csnumber=41921

C-TPAT, 2001	US	CBP	From any country to US (import)	All	6375 certified and 3916 validated companies	Govt. voluntary	SCS
CSI, 2002	US	CBP	Applied to Imports to US	Sea	58 ports	Govt. Voluntary	SCS
WCO SAFE FoS, 2005	WCO	WCO	Worldwide	All	156 Members States	Intl. Voluntary	Standards for SCS and trade facilitation
ISO28000 Series, 2005	ISO Technical Committee	ISO	All	All	157 member countries	Intl. voluntary	Improve SCS
EU-AEO, 2008	European Commission	DG Taxation and Customs	Any country to EU import, export	All	192 companies	Govt. voluntary	Trade facilitation and SCS

2.5 Major Regional and National SCS programs

For the interested reader, the list of these programs is in Annex III.

2.6 Other significant SCS programs/projects

2.6.1 Operation Safe Commerce (OSC) (2002)

Operation Safe Commerce (OSC) is a collaborative effort between the US government, private business and the maritime industry, to develop and share best practices for the safe and expeditious movement of containerized cargo. New technologies and initiatives are being implemented in selected global supply chains. These are aimed at improving security during the process of stuffing and deconsolidating containers, physically securing and monitoring containers for transportation, and exchanging timely and reliable communication.

Phase II of OSC consisted of 18 pilot projects designed to improve container SCS. More specifically, the project identified and implemented commercially viable business processes, technologies and initiatives to protect commercial shipments from threats of terrorist attack, weapons of mass destruction, smuggling and contraband, while minimizing the economic impact on the transportation system. This project analyzed existing practices and tested security techniques in an operational intermodal transport environment.

Inspections, data collection and transmission activities were performed as follows:

- New security techniques for inspecting goods at point of origin
- Independent verification of the integrity and electronic tracking of the container and data throughout the supply chain
- Transmission of secure electronic data to a data clearing.

2.6.2 EU-China: Smart and Secure Trade Lane Pilot Project (2006)

During the second session of the Joint EU-China Customs Cooperation Committee (JCCC) meeting on 19 September 2006, the EU and China reached an agreement to initiate this pilot Project. The initial motivation and longer-term goal is that the two sides (EU and China) will give mutual recognition of each other's security

standards and AEOs, and collaborate to improve information exchanges and risk assessment by means of the latest technologies aiming at ensuring smooth and prompt Customs clearance. It is hoped that the Smart and Secure Trade Lane Pilot project will permit tests of "end to end supply chains" from the point in time when a container is loaded through its entire journey up to its final destination. Currently the project is a cooperation project between the EU Commission, the Customs authority in China and the Customs authorities in UK and the Netherlands. However if the pilot project is successful, it will be progressively extended to cover the whole EU and more ports in China. An evaluation for this pilot project is scheduled for completion in 2009.

2.6.3 US Secure Freight Initiative (SFI) (2006)

In December 2006, the US government's DHS and Department of Energy launched the SFI initiative that aimed at strengthening the ability of the American authorities to trace nuclear and other radioactive substances at borders. This program is considered by the US as a laboratory and testing phase for the ultimate goal of 100 % scanning. Since 2007 the latest technological equipment has been placed in seven foreign test ports: Port Qasim in Pakistan, Puerto Cortés in Honduras, Southampton in the UK, Salalah in Oman, Singapore, Busan in South Korea and Hong Kong in China. According to the US CBP: "The International Container Security project strengthens maritime cargo security and global nuclear non-proliferation efforts by providing real time radiographic and spectrographic scanning of maritime shipping containers. It adds a new dimension to be significant technological advancements by integrating those data elements into the US Customs and Border Protection (CBP) process".[26]

The further ambition is to develop a globally integrated network of radiation detection and container imaging equipment to be operated in seaports worldwide. This network should allow streaming scanning images and radiation detection data for verification in the US. The arrangement is that this data will be shared by governments across the world and the government of the US. An additional feature is the development of a new risk scoring feature, partly based on existing, but uncollected data.

2.6.4 Columbus Program

Following the acceptance of the SAFE Framework, the WCO started in 2006 what is termed the Columbus Program, which is specially designed to help Members, especially those from developing countries, implement the SAFE Framework and related international obligations, such as the WTO negotiations on trade facilitation. The program is the largest and most comprehensive Customs capacity building to date. The Columbus Program consists of three phases:

- The 1st phase, needs assessment, is a comprehensive diagnostic needs assessment of the current situation in the Customs administration uses the WCO's Diagnostic Framework tool that has been acknowledged by organizations like the UN, OECD, the World Bank, the International Monetary Fund (IMF) and others. The needs assessment diagnosis is carried out by two capacity building experts. During the diagnostic mission, the experts interview all concerned parties including the members of the trade community. The mission results in a diagnostic report including the current situation, gap analysis to full implementation and the suggested way forward through a number of recommendations

[26] This section is based primarily from information obtained from the U.S. Customs and Border Protection document titled Secure Freight Scanning at a Glance., available at http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/trade_security/sfi/sfi_scanning.ctt/sfi_scanning.pdf

- The 2nd phase, Implementation, is support for action planning, donor matchmaking, planning of pilot activities and implementation.
- The 3rd phase, Monitoring, involves monitoring of progress. The Capacity Building Directorate has developed a progress monitoring system that was presented to and endorsed by the WCO High-Level Strategic Group in Shanghai. Progress reporting will be made on a country level, on a regional level and will involve donors.

At the time of this writing, over 100 diagnostic needs assessments have been undertaken or are scheduled. 69 Phase 2 national missions and 14 Phase 2 regional missions have been completed.[27]

2.6.5 China Customs-company classification program (2008)

Launched on 1 April, 2008, by the Chinese General Administration of Customs, this program covers imports and exports involving China, in all forms of transport. The goal is for the Chinese Customs to classify importing and exporting companies on the basis of their security compliance and historical record with Customs. Classes are AA, A, B, C, and D. AA and A class companies enjoy advanced Customs privileges, such as limited inspection risk, quick inspection protocols and quick release. Class AA companies enjoy electronic communication and declaration procedures, without, for example, the need to submit paper documents.

2.6.6 GTX or Global Trade Exchange

GTX was an initiative launched by the US Department of Homeland Security (DHS) in 2007, as a government-controlled, privately operated, user-fee based data warehouse that would have taken the huge quantities of trade data and made this available to the US government and other governments in order to improve supply chain security. Under mounting pressure from the trade community due to data dissemination issues, in April 2008, the US Customs and Border Protection announced that the GTX initiative would be suspended.

2.6.7 ACE or Automated Commercial Environment

"The Automated Commercial Environment (ACE) is the United States' commercial trade processing system designed to automate border processing to enhance border security and foster our Nation's economic security through lawful international trade and travel. ACE will eventually replace the current import processing system for U.S. Customs and Border Protection (CBP), the Automated Commercial System (ACS). ACE is part of a multi-year CBP modernization effort and will be deployed in phases. ACE provides a solid technology foundation for all border security initiatives within CBP and will:

- *Allow trade participants access to and management of their trade information via reports*
- *Expedite legitimate trade by providing CBP with tools to efficiently process imports/exports and move goods quickly across the border*
- *Improve communication, collaboration, and compliance efforts between CBP and the trade community*
- *Facilitate efficient collection, processing, and analysis of commercial import and export data; and*
- *Provide an information-sharing platform for trade data throughout government agencies."*[28]

[27] This information is based primarily on information obtained from the WCO website;
http://www.wcoomd.org/home_wco_topics_cboverviewboxes_programmes_cbcolumbusprogrammeoverview.htm
or more information go to
http://www.wcoomd.org/home_wco_topics_cboverviewboxes_programmes_cbcolumbusprogrammeoverview.htm

[28] ACE 101 – Department of Homeland Security, Customs and Border Protection
http://www.cbp.gov/linkhandler/cgov/trade/automated/modernization/ace/ace101.ctt/ace101.pdf

2.6.8 LRIT or Long-Range Identification and Tracking of ships[29]

"The Long-Range Identification and Tracking (LRIT) system provides for the global identification and tracking of ships. The obligations of ships to transmit LRIT information and the rights and obligations of Contracting Governments and of Search and rescue services to receive LRIT information are established in regulation V/19-1 of the 1974 SOLAS Convention.

The LRIT system consists of the ship borne LRIT information transmitting equipment, the Communication Service Provider(s), the Application Service Provider(s), the LRIT Data Centre(s), including any related Vessel Monitoring System(s), the LRIT Data Distribution Plan and the International LRIT Data Exchange. Certain aspects of the performance of the LRIT system are reviewed or audited by the LRIT Coordinator acting on behalf of all Contracting Governments.

LRIT information is provided to Contracting Governments to the 1974 SOLAS Convention and Search and rescue services entitled to receive the information, upon request, through a system of National, Regional, Cooperative and International LRIT Data Centers using the International LRIT Data Exchange. (…)".[30]

LRIT applies to the following vessels (international movements):

- Cargo vessels (300 gross tons and above, with high speed included)
- Passenger vessels (high speed included)
- Offshore drilling platforms (mobile only).

At least four times per day the vessels must report their position to the administration which is associated with the flag of that vessel.

When used in conjunction with the short range Automatic Identification System (AIS), LRIT can be considered to be an integral layer in the supply chain security tracking and tracing process.

However, LRIT seems to experience some difficulties concerning the proper control and dissemination of LRIT information by flag states, port states and coastal states when it comes to prevent that critical LRIT information reaches the hands of malevolent parties who might use it to attempt to spot and trace vessels (see AIS below).

2.6.9 AIS or Automatic Identification System[31]

Vessel Tracking Services (VTS) and ships use the Automatic Identification System (AIS) for locating and identifying ships within a relatively limited range. When AIS is combined with the Long Range Identification and Tracking (LRIT) system, this provides a clear tracking and tracing layer in supply chain security. Practically, the AIS enables vessels to transmit receive and share real-time data covering ship identification, positioning, course, and speed. Additionally, vessels tracking services and maritime authorities can use this information to monitor and control vessel movements accordingly. According to the IMO SOLAS convention AIS must be installed on all passenger ships and cargo ships over 300 gross tons.

[29] LRIT is actually a compulsory system for the long-distance tracking of vessels. It is listed in the "other significant SCS programs", because it is functioning at vessel level, and does not require specific action on the part of the transport & logistics actors, other than ship-owners and maritime authorities.
[30] http://www.imo.org/includes/blastDataOnly.asp/data_id%3D24242/overview.pdf
[31] AIS is actually a compulsory system for the short-distance tracking of vessels. See remarks in notes 6 & 29.

"Although AIS is an important step forward in monitoring vessel traffic, its existence places vessel information in the hands of anyone who has an AIS receiver. Pirates in the Gulf of Aden, for example, have been known to have used AIS information to improve their ability to intercept and hijack vessels. The problem of securing the AIS systems against outsiders' acquisition of information that can be used to compromise the safety or security of the vessels remains to be urgently solved".[32]

2.6.10 MDA or Maritime Domain Awareness

Maritime Domain Awareness is the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States.

MDA Goals

MDA supports core national defense and security priorities over the next decade. MDA serves to simplify today's complex and ambiguous security environment by meeting the following strategic goals:

- Enhance transparency in the maritime domain to detect, deter and defeat threats as early and distant from U.S. interests as possible
- Enable accurate, dynamic, and confident decisions and responses to the full spectrum of maritime threats; and
- Sustain the full application of the law to ensure freedom of navigation and the efficient flow of commerce.

MDA Objectives

Achieving MDA depends on the ability to monitor activities in such a way that trends can be identified and anomalies differentiated. Data alone are insufficient. Data must be collected, fused, and analyzed, preferably with the assistance of computer data integration and analysis algorithms to assist in handling vast, disparate data streams, so that operational decision makers can anticipate threats and take the initiative to defeat them. The following objectives constitute the MDA Essential Task List, which will guide the development of capabilities that the United States Government will pursue and when executed will provide the GMCOI an effective understanding of the maritime domain and allow for continuous monitoring:

- Persistently monitor in the global maritime domain:
  - Vessels and craft
  - Cargo
  - Vessel crews and passengers
  - All identified areas of interest
- Access and maintain data on vessels, facilities, and infrastructure
- Collect, fuse, analyze, and disseminate information to decision makers to facilitate effective understanding.

Access, develop and maintain data on MDA-related mission performance.[33]

[32] Source World Shipping Council 2008

[33] National Plan to Achieve Maritime Domain Awareness for The National Strategy for Maritime Security - October 2005 (USA)

Table 2-4 Summary of other significant SCS programs/projects

Name/Year started	Originated Country/ Institute	Regulating body	Covered route	Transport mode	Participation/ Status	Category	Goal
OSC, 2002	US	DOT	Highways and railways in the US	Containers	Pilot project	Govt.– Voluntary	To enhance container supply chain security
EU-CHINA Smart and Secure Trade Lane Pilot Project, 2006	Joint EU – China Customs Coop	EU and China Customs	Initially involves Rotterdam (NL), Felixstowe (UK) and Shenzhen (China)	Initially the Sea ports	Pilot project	Govt.- Voluntary	Mutual recognition and smooth and prompt Customs clearances
SFI, 2006	US	DHS	From any country to US (Import)	Containers	Pilot phase	Govt.- Voluntary	Strengthen US ability to trace nuclear and other radioactive substances at borders
Columbus Program, 2006	WCO	WCO	Worldwide	All	101 diagnostic missions, 73 country and regional implements	Int. Voluntary	Assist developing countries implement SCS measures; particularly WCO
China Customs Company Class. program, 2008	China	China Customs	From any country to China (import)	All	Unknown	Govt.- Voluntary	Classify importing and exporting companies on the based on previous security compliance

2.7 Discussion and Conclusion

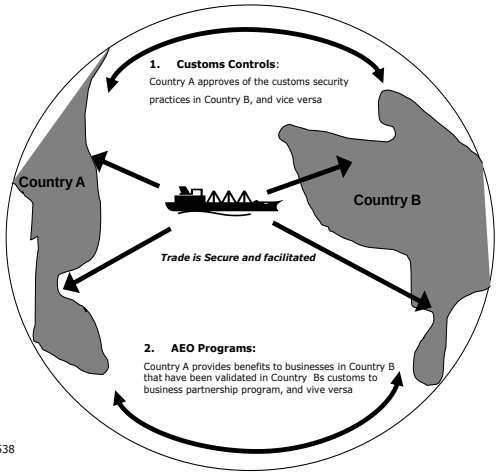
2.7.1 Mutual Recognition

A common issue most states and other actors are united upon is how to harmonize all the regional or national initiatives and to work towards mutual recognition of the certification programs. The purpose of this is to avoid that a supply chain actor who has been certified in one country has to duplicate the effort of becoming certified by other countries standards and procedures. This is what is called “mutual recognition”. Mutual recognition is seen as beneficial, as it simplifies procedures between customs through recognition of each other’s standards. Coordination is, moreover, seen far more appealing than the confusion induced by conflicting overlapping or contradicting programs. That is not to say that all actors are in full agreement with the specific details of each program - in many cases only a few requirements correspond to those requirements of another program, and in some cases almost all requirements correspond. While the ideal of Mutual Recognition is therefore not an issue, the *real issue* is focused on what different programs’ actors prioritize at the expense of what others see as important, and vice versa. This is where the issue of mutual recognition becomes difficult. For example, EU AEO has placed greater emphasis on trade benefits ahead of security; whereas the US C-TPAT program places greater emphasis on security over trade.

A major exponent of the benefits of mutual recognition is described by the WCO in their document titled the SAFE Framework, which was published in June 2005. The document calls upon Customs administrations to work with each other to develop mechanisms for mutual recognition of AEO validation/authorization and Customs controls, in order to eliminate or reduce redundant and duplicated efforts, as illustrated by figure 1.3 below. The WCO SAFE Framework advocates a risk management approach to global supply chain, with one of the main goals being to establish a network of mutual recognition of AEO programs, which allows two or more countries to rely on each other's security regimes to ensure any cargo shipped between them is free of threats. Under this framework, countries would establish their own cargo screening and scanning regimes and manage them at a commonly accepted level set by the WCO.

Mutual Recognition is a concept where an action or a decision taken by a party authorized by one Customs administration is recognized and accepted by another Customs administration. This should include security audits.

Figure 2-4 Two forms of Mutual Recognition



Source: GAO-08-538
August 2008

pppBeyond AEO status, the next step is the recognition of the AEO status granted to an economic operator in one country by the Customs administration in another country. This means that the Customs administration in a second country has accepted both the Customs controls and the Customs AEO validation in the first country. The process of mutual recognition gives the economic operator granted AEO status in one country, and also the AEO status and benefits in another country without having to repeat the validation procedure. The EU has enshrined AEO status and its benefits in the new EU Customs Code.

The US C-TPAT, Canada's PIP, Jordan's Golden List, Singapore's STP, Japan's AEO program and New Zealand's SEP are examples of AEO programs that offer trade facilitation benefits to economic operators who secure their supply chain (see Annex II). So far, however, the progress of AEO mutual recognition has been slow, although Customs authorities globally are continually working to achieve mutual recognition for their programs so that holders of one can enjoy some or all of the benefits of the other programs.

One major question in this area is how and when will foreign AEOs be recognized as US C-TPAT compliant, (the AEO equivalent in the US). When comparing CTPAT with EU AEO certification, there are several similarities as both contain a significant security element, both deal with the import of goods and both offer significant customs advantages to compliant members. Indeed in March 2006, a joint roadmap towards mutual recognition of C-TPAT and AEO was adopted and the target for implementation is in the year 2009. Beyond the professions of goodwill, one still can hear nuanced if not diverging voices on the issue on both sides of the Atlantic.

2.7.2 The need to assist developing countries with SCS Program Implementation

As seen in the above listed programs, most programs have their origin in the developed world. To a large extent, many of these programs have been implemented without much consideration on how developing countries feel about the programs, or whether they are able to meet such standards.

An exception to the above is the Columbus Program of WCO. Due to the wide range of activities undertaken across some 100 countries, it offers extensive data sets from which conclusions can be drawn concerning the specific needs of developing countries, and specifically the real and possible barriers to effective national implementation of global policy initiatives. The WCO analysis of the results of phase 1 of the Columbus program has exposed a wide range of developmental needs among its Members, ranging from those countries with minimal developmental needs and no requirement for external capacity building assistance, through to those needing comprehensive technical assistance and capacity building assistance. In between these two extremes are countries which have already created the fundamental infrastructure requirements, but need specific training and technical support, some of which also require support with policy development and change management support. The fact that such comprehensive and, in some cases, quite basic developmental needs have been recognized in relation to this particular international regulatory framework is important. These findings identify not just the need for extensive capacity building support requirements in order to implement the WCO SAFE Framework, but also the possible inability of many countries to successfully implement the hundreds of conventions, agreements and guidelines to which they have given an international commitment without, for one, receiving significant capacity building assistance. The WCO, similarly, recognizes this in its conclusion, in which it indicates the need for a different approach to capacity building assistance in the future (WCO 2006):

The support that is needed will change. The WCO will have to put more resources into planning, recruitment of experts, donor matchmaking, the development of management skills and skills to handle modernization (like e.g. project management, reform management, tendering/contracts, monitoring, ICT and technical specifications, etc.).

In this regard, K. Mikuriya (2008), WCO Secretary General, remarks: '*While the technical area of procedures, infrastructure and technology remains important, sustainable capacity building also requires change management … including a change in culture*'. Already recognizing this, the WCO has begun to advance a number of these initiatives through its Partnership in Customs Academic Research and Development (PICARD) program. In particular, the development of management skills has been addressed in a way which seeks to establish internationally consistent development standards that are designed to maintain and raise the academic standing of the customs profession. According to the WCO (2008), the primary objective in developing such standards is to 'establish benchmarks which can be developed into job profiles for the purposes of customs recruitment; against which the in-house training of member administrations may be measured; and against which academic development can be designed or procured'. The resultant standards, WCO 2008, are now being used to develop educational programs which provide internationally recognized professional qualifications for customs professionals from both the public and private sectors.

While considerable progress has been made by the international community in relation to the establishment and agreement of standards, there is a long way to go to guarantee that the respective countries have the required capability to translate the theory into practice. The exercise carried out by the WCO shows that consistent global application of existing and future conventions, agreements and guidelines relating to border management is improbable without significant capacity building assistance.

2.7.3 Conclusion

This Chapter was intended to give the reader a sense of the multiplicity and diversity of SCS "initiatives" and programs around the world. It has attempted to shed some light on this profusion of activities, concepts and schemes, in particular by clarifying what is compulsory, what is not, and what might become compulsory and when.

It has also tried to highlight features which, though not compulsory by law, can impose themselves in one form of another upon the actors of international trade by certification programs, thus becoming effectively de facto law. Here, the propagation of ISO-certification might serve to illustrate how programs can become international standards and what is in store for traders and transporters. Originally, the ISO 9001 Quality Management Standard certification took a long time to spread, and, in its beginning, many were not heeding these developments. It has however slowly imposed itself through market pressure, with more and more clients demanding ISO-certification from their suppliers, starting, in the logistics industry, with the transport, handling and storage of hazardous cargo, then moving on to high-value cargoes, to eventually become gradually more and more demanded due to its perceived benefit of "quality insurance" in the chain of transport providers. Similarly, the first AEO-like certification program was launched by the US government in the wake of 9/11, under the name C-TPAT in 2001. Gradually the AEO concept has also spread to the point now that AEO certification programs are seen in the EU and are being advanced in other parts of the world. Significant efforts have been deployed by the WCO to alert and prepare developing countries that these initiatives will too encompass them sooner or later in terms of compliance or adhesion to SCS programs. Problematically, it was found that a greater assistance needs to be given to developing countries to prepare them to this eventuality.

3 SUPPLY CHAIN SECURITY TECHNOLOGIES

The global supply chain is a distribution enterprise by nature. As such, it needs transport modes (land, air, and sea) and transfer points, like maritime ports, air ports and inland transport facilities. In addition to the programs, policies and procedures outlined in the previous chapter, the supply chain also requires the use of technologies. Since operators in the supply chain are in the business of moving goods, protecting those goods from loss, theft and tampering is also inherently part of what these operators must address.

While the basic concept of security has changed little over time, there is now a trend to serve two purposes: security and efficiency. This collaboration between security and efficiency specialists actually began as a concept over 50 years ago. In 1956, it was a truck company owner driver who changed the shipping industry. Malcolm McLean observed a slow, inefficient and non-secure process for 20 years before he developed a container to secure his freight and move it in an efficient manner. This container standardized security, lowered costs of trade, lowered in-transit losses, and allowed for interoperability. Today the container is still the center of the focus of SCS.

While this chapter will focus on the new technologies applied in SCS it will also display that the human component cannot be ignored. The issues of cost absorption will continue to be a problem for the developing world if new SCS schemes and legislature dictate technology use.

This chapter will review emerging and existing technologies; container integrity (CI), track/trace efforts, Advanced Inspection (AIT). Due to space constraints, information and communications technology (ICTs) , and technologies used to actualize data models, and two other collaborative tools, Electronic Single Windows (ESW) and Port Community systems (PCS) used in the supply chains will not be analyzed in detail. They are only mentioned in this introduction. They are not core to SCS, but, by nature, can contribute to its enhancement. For the reader interested in ESW and PCS, it is recommended to read: United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) Recommendation nr 33[34].

3.1 Emerging trends in technology

In reviewing the numerous SCS schemes outlined in Chapter 1, most consider the container to be the main focus of security. It seems to make perfect sense to address the security issues linked to container technology once the consequences of a Trojan horse scenario or smuggling threats and crimes are analyzed. With that said, containers or containerized intermodal transport is not the only target. The global supply chain relies on various loading units or conveyances. Pipelines, bulk, roll on/roll off are all susceptible to, and have suffered interdiction on many occasions. In fact, according to most statistics available today, approximately 85% of loss within the supply chain occurs during hinterland transport. As world trade volumes continue to multiply and borders become more open, criminal and terrorist networks have become more organized and sophisticated. One avenue explored to combat the increased technology use in the modus operandi of criminal elements; so-called “smart containers” have been developed. Today’s “smart containers” include a navigation and routing guidance system, satellite location, interior sensors, and radio frequency identification to secure the box from origin to destination. It can be estimated that a few thousand “smart containers” are in use at the time of the

[34] http://www.unece.org/cefact/recommendations/rec33/rec33_trd352e.pdf

first publication of this guide. The world-wide fleet of containers currently in use consists of 16 million units (24 million TEUs)[35].

"Smart containers" sensors can detect anomalies such as:

- Door opening or removal
- Cutting of holes in the roof, sides or floor
- People or animals inside, e.g. by using passive infrared sensors
- Dangerous chemical, biological or radiological material, e.g. by using CBRNE sensors
- Location, e.g. using GPS or Galileo– for track and/or trace applications.

The sensors would be connected to some form of central data logger. Sensor data from the logger could either be read at a port or border crossing point equipped with a compatible seal reader, or is sent by a long range communication system, e.g. satellite or GSM, to a monitoring point. So far, there are varying claims of benefits to the private sector for using "smart containers" and their associated technologies and systems.

The following synopsis by Giermanski (2008) highlights the potential of the "smart containers":

"smart containers" have already been demonstrated to work. In 2006 between Germany and the US it was shown that the cost to the shipper is minimal, hardly more than electronic locks and seals…"smart containers" can carry and transmit electronically both logistics and sensory data. While there is no single definition of a smart container, it should be defined generally as a conveyance that meets World Customs Organization standards and complies with U.S. law, like the SAFE Port Act, and U.S. programs like C-TPAT by carrying and transmitting electronically, data and security intelligence from origin through destination to Customs when needed and on demand. "smart containers", as they exist today, perform at least seven clearly defined operations:

1. *Functioning as a part of a system approach necessary to coordinate all facets of the supply-chain process to ensure visibility and security, beginning at origin*
2. *Capturing and transmitting electronically certain trade data that will link to other supply-chain documentation. Examples would be the container number, or booking number*
3. *Complying with the WCO, C-TPAT and the European Union's Authorized Economic Operator requirements to maintain the integrity of the entire container, by detecting a breach anywhere into its body*
4. *Reporting any breach in real time or close to real time*
5. *Providing worldwide geographic positioning throughout the supply chain when queried, and when programmed, automatically report its position if it is off its designated course of travel*
6. *Recognizing and recording the identity of the authorized person opening the container at destination*
7. *The container should be adaptable to different sensors and be able to communicate with or be adapted to divergent software packages used by shippers and carriers within the supply chain".*

Some in the industry, however, regard so-called "smart containers" more as a miracle cure promoted by some technology providers. It has been commented that a container will never be smart, regardless the amount of technology propped into it. It is also argued that some of the "live tests" conducted so far have been nursed and cocooned from end to end, and would probably find it hard to routinely survive real life stress.

[35] By end 2007

Container transportation, by nature, is heavily standardized (see ISO norms for maritime containers) and commoditized. Introducing a segregation between “smart” and “non-smart” containers, in itself, could be a challenge.

Initially, “smart containers” would be owned by the shippers who have a specific use for them, and treated as “shippers owned” by the sea-carriers. This entails the problem of returning them to origin when emptied. Some container leasing companies have started to offer such equipment to lessees. Another avenue being explored, probably more viable, is to have removable “smart kits” that can be affixed onto any standard container, in a way somewhat similar to flexi-tanks or remote reefer cargo probe sets.

These “smart kits”, sometimes called Asset Monitoring Unit (AMU), Container Monitoring Unit (CMU) or Asset Protecting Unit (APU) , depending on the vendor, derive much of their technology, methodology and general philosophy from the high-tech “supply chain visibility” line of thought, which addresses tight inventory management issues. Some types of cargoes indeed do justify, and can afford a much closer attention than ordinary cargo, such as high-value cargo, pharmaceuticals, sensitive chemicals, military supplies, and fashion goods linked to promotional campaigns do indeed resort to this kind of high-visibility devices, generally provided by the logistics operators. On the other hand, while ordinary Importers would also enjoy the extra level of 24/7 visibility service, there is no sign in the market that they even remotely appear interested in paying for it.

Biometrics is also being introduced to the supply chain. Driver identification and verification is an essential function at cargo pickup points, intermediate delivery terminals, and even at destinations. Biometrics can improve the effectiveness of the function, reducing the risks of theft and terrorism while facilitating gate and reception processes, especially for drivers who make frequent pick-ups and drop-offs at the terminal. Biometric identification tools, such as fingerprint and iris recognition, may be incorporated in smart identification (ID) cards and integrated with on-line access to manifest, vehicle, and driver databases. Looking ahead, the Transportation Security Administration (TSA) Transportation Worker Identity Card (TWIC) aims to deploy a common biometric smart ID card for all US transportation workers.

3.2 Existing technologies

The following sections will provide a brief overview on the different types of technology used in SCS and how they are applied. While a complete overview of all existing technologies available on the commercial market would be beneficial to the readers of this guide, a current catalogue is available online with the WCO. The WCO maintains, for the benefit of its 174 Members, a Databank on Advanced Technology accessible via the Organization’s website. The Databank assembles information on technical equipment available in the market place and provides detailed and updated information of currently available technologies listed such as:

- Test & detection equipment
- X-Ray equipment
- Mechanical and electrical container seals.

3.3 SCS Technologies for Container Integrity: Container security devices and seals

Container Security Devices (CSD) play a crucial role in ensuring the integrity of the container along the supply chain and facilitating trade and Customs processes. Cargo security can be enhanced through the use of both mechanical and electronic seals. Both mechanical cargo seals and e-Seals act as barriers against pilferage, smuggling, and sabotage of cargo within containers and trailers en route to their destination. If either type of

seal is found to be broken or if its identification (ID) number is different from the one on the cargo document, this is an indication that the container or trailer door might have been opened by an unauthorized person at some point in the transportation route. The unique ID numbers on both mechanical and e-seals provide tracking information. It is expected that the ID number on either type of seal will be recorded at each handoff in the chain of custody to provide information about when and where the container or trailer was handed over and the seal status at that time.

Ideally, seals should only be placed on containers by the party directly responsible for stuffing and/or visually verifying the contents of the container. In this respect, it should be stressed that the party responsible for stuffing and sealing the container is the first, and most important, link in a "secure" container transport chain. One must however remember that even high-security mechanical seals are only as good as the procedures in place to affix, monitor and document them at each transfer of responsibility.

3.3.1 Mechanical Seals

For the purposes of this document, the following terms and definitions from ISO 17712 apply. The classifications and types are outlined below.

A mechanical seal is a device marked with a unique identifier and is often marked by the seal owner's or issuer's stamp and/or color. It is externally affixed to the container doors and designed to evidence tampering or intrusion through the doors of a container and to secure closed doors of a container. In addition, depending on its construction, the seal provides varying degrees of resistance to an intentional or unintentional attempt to open it or to enter the freight container through the container doors. Even if a tampered seal were to be replaced with a similar unit after entry, the seal's unique identification number might not match with the one that was recorded when the original seal was affixed. The sealing process for security seals is as important if not more important than the seal itself.

Proper sealing protocols are comprised of a number of elements including the following:

- Purchasing/sourcing and shipping procedures for seals
- Training in seal use and verification
- Tracking of seal inventories and safe storage/release procedures
- Correct application of seals
- Recording seal numbers
- Managing and transmitting seal numbers
- Recording seal operations and identification of people involved and time and date
- Recording seal anomalies
- End-of-use and end-of-life disposal of seals.

Without proper sealing and checking protocols, the use of seals can be counter-productive as they can instill a false sense of security as to the status of the container handle/door. In theory, security seals should prove effective in detecting any attempt to tamper with the container.

In reality, however, simple security seals are relatively easy to defeat. The reasons are numerous but include the ease with which they can be cut, the possible lack of proper seal documentation, the possibility of poor security management in the container transport chain and the relative ease of replicating certain seals and their numbers. As with simple indicative seals, verifying the seal is both a manual and time-consuming process and thus many seals are only summarily checked, if checked at all, while in transit. Finally, and this is not a

problem unique to security seals, experienced thieves have devised ways to bypass the handle or the container doors entirely when gaining entry to the container.

One must however always remember that even high-security mechanical seals are only as good as the procedures in place to affix, monitor and document them every time the container changes hands (at each transfer of responsibility).

In addition, once illegitimate cargo stealthily finds its way into a container prior to affixing the seal, the sealed container will be as good as a legitimate passport all the way to destination. This is why upstream supply chain security procedures must include the company, personnel and facilities that produce, pack and stuff the cargo into the container.

3.3.1.1 Types of mechanical seals

High security seals

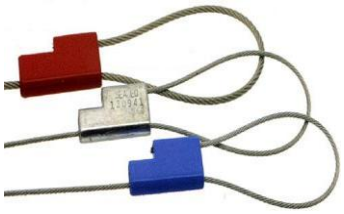
This is a seal that is constructed and manufactured of material, such as metal or metal cable, with the intent to delay intrusion. High security seals generally must be removed with quality bolt cutters or cable cutters. They require inspection to indicate whether tampering has occurred or entry has been attempted. According to the 9/11 Commission Act of 2007, effective October 15, 2008 all containers in transit to the United States shall be required to be sealed with a seal meeting the International Organization for Standardization Publicly Available Specification 17712 (ISO/PAS17712) standard for sealing containers. It is crucial that companies are aware that all cargo arriving by vessel at any port of entry in the United States are required to be sealed with a seal meeting the ISO/PAS 17712 standard for High Security seals. The WCO has also endorsed the ISO 17712 standard for seals.

There are many types of seals on the market that meet or exceed the ISO 17712 standard and many seal manufacturers. Businesses are responsible for acquiring seals from legitimate manufacturers. Companies purchasing seals should be backed by the seal manufacturer's test report issued by an independent ISO17025 certified testing laboratory. Businesses should maintain this documentation for future reference. While this guide does not endorse any particular seal manufacturer or product, there are organizations, such as the International Seal Manufacturers Association (ISMA) that can provide information on seal manufacturers offering ISO PAS 17712 high security seals.

A variety of High security Seals is shown below:

Padlock seal: Locking body with a bail attached: either wire shackle padlock (metal or plastic body), or plastic padlock and keyless padlock seals.

Cable seal: Cable and a locking mechanism. On a one-piece seal, the locking or seizing mechanism is permanently attached to one end of the cable. A two-piece cable seal has a separate locking mechanism which slips onto the cable or prefabricated cable end.



Bolt seal: Metal rod, threaded or unthreaded, flexible or rigid, with a formed head, secured with a separate locking mechanism

Barrier seals: Designed to provide a significant barrier to container entry. A barrier seal may, for example, enclose a portion of the inner locking rods on a container. Barrier seals may be designed to be reusable.

Security seals

Seal that is constructed and manufactured of material that provides limited resistance to intrusion and requires lightweight tools for removal. Security seals require inspection to indicate whether tampering has occurred or entry has been attempted.

- Wire seal: length of wire secured in a loop by some type of seizing device. Some examples are crimp wire, fold wire and cup wire seals.

- Strap seal: metal or plastic strap secured in a loop by inserting one end into or through a protected (covered) locking mechanism on the other end

Indicative seals

Seal that is constructed and manufactured of material that can easily be broken by hand or by using a simple snipping tool or shear. Indicative seals require inspection to indicate whether tampering has occurred or entry has been attempted.

- Cinch or pull-up seal: indicative seal consisting of a thin strip of material, serrated or non-serrated, with a locking mechanism attached to one end. The free end is pulled through a hole in the locking mechanism and drawn up to the necessary tightness. Cinch or pull-up type seals may have multiple lock positions. These seals are generally made of synthetic materials such as nylon or plastic. They should not be compared to simple electrical ties



- Twist seal: steel rod or heavy-gauge wire of various diameters, which is inserted through the locking fixture and twisted around itself by use of a special tool.
- Label or Tape seal: These seals are self-adhesive and self-voiding seals. They are used as an adjunct security protocol on doors for any container. They are hand applied by removing the protective paper backer and sticking them to the container over or under the keeper bars. They are used to visually indicate tampering or opening of the doors while unattended. These seals work as a silent sentry to monitor doors where bolt seals, plastic seals or other conventions seals cannot. Bolts or any seals placed in a normal right hand seal hole are easy to circumvent.
- Tape door seals are manufactured with barcode, coated with anti counterfeiting components. This application procedure will indicate if the doors had been removed. These seals are easy to visually interrogate and they provide a formidable barrier to thieves against surreptitious entry. As a chain of custody tool, anyone seeing them violated will immediately know with little or no training.

3.3.2 Electronic Seals

The need to further secure containers containing high value goods has led to the development of several types of so-called “smart” seals. These types of seals have integrated physical security and information management capabilities. It is the latter functionality that sets these aside from their mechanical counterparts since they can transmit data regarding their status as well as the information regarding the contents of the container. At a minimum, an electronic seal system combines a physical sealing device with a data chip capable of recording and restituting basic information regarding the container contents, such as an electronic cargo manifest, and a mechanism for reading the information recorded on the chip. A higher level of functionality is added by systems capable of electronically communicating whether the seal has been broken or otherwise tampered with. These seals use radio frequency (RF), infra-red (IR) or fiber optics to transmit data. In their most advanced iterations, electronic seals can be coupled with a variety of sensors (e.g., radioactive, radiological, chemical, biological, light, CO2, etc.) that can record and communicate data regarding the in-container environment. In combination with a global positioning system (GPS) transceiver, alerts or status messages regarding the container can be transmitted in real time to a central processing system that can pinpoint the container’s location. The following section on e-seals is outlined in the Organization for Economic Co-operation and Development and European Conference of Ministers of Transport *Container transport security across modes* (2005).

What do e-seals monitor?

E-seals only monitor the seal's status and that of any sensors connected to the seal – they do not monitor the condition inside the container. This nuance is important. As pointed out earlier, a container's integrity can be compromised without compromising the integrity of the seal. Even when sensors are attached, the seal records sensor events which may or may not reflect what is actually happening within the container environment. "False-positive" readings from sensors are a particular concern but one should not overlook the possibility that sensors can be defeated by more or less sophisticated means.

What do shipping-related information e-seals provide?

E-seals cannot provide detailed information on the contents of a container. What they do provide is information regarding what the party responsible for sealing the container said was in the container. If that party was an originating shipper, one might assume that the information is more or less correct. However, if that party is once or twice removed from the originating shipper like in the case of a carrier placing an e-seal on a container that arrived at the terminal with a non-conforming mechanical seal, then the shipping documents loaded into the seal's memory only reflect the e-seal-affixing party's best available information as to the contents of the container. In a worst case scenario, a conforming e-seal on a container containing illegitimate cargo might actually facilitate the transport of that cargo, rather than prevent it. Non-declaration or mis-declaration of goods is not an unknown phenomenon in international transport, and the catastrophic outcomes of certain incidents such as mislabeled calcium hypochlorite or fireworks-containing containers, highlights both the reality and the risk of such situations. Any sense of security instilled by the presence of an e-seal on an intentionally mis-manifested container containing a WMD would have dramatic consequences.

E-seal infrastructure

For e-seals to be an effective part of a global container security strategy, they must be accompanied by a host of reading devices/scanners, computer hardware and a suite of underlying information management software systems capable of properly processing the seal data. Today, these requirements are far from being met, and their fulfillment throughout the container transport chain is not at all assured in the near future. It is likely that major terminal operators will be the first to place e-seal readers at strategic locations within their container terminals and to use such systems to monitor and track the status of such seals. Some of the major maritime carriers might start to deploy e-seal readers as well. However, it is not at all sure that smaller ports will be able to deploy and effectively manage such systems in the medium term. Furthermore, while it is feasible that major railroads and barge operators might also be able to deploy the underlying infrastructure and hardware necessary to support e-seals, it is highly unlikely that small road carriers and smaller barge/rail operators will be in a position to do so any time soon – if ever. What is likely to emerge is uneven support for e-seals across the container transport chain with certain high security nodes capable of processing e-seal data punctuated by areas of low or no e-seal functionality. Properly identifying the boundaries of these zones and developing appropriate container transfer protocols among these zones are necessary components of a comprehensive container security plan.

Types of E-seals

There are four types of e-seals, classified by the four different communication systems used between the seal and its "reader:"

- Radio frequency identification (RFID)
- Infrared (IR)
- Direct contact, and
- Mobile GSM or satellite.

The following data is provided by the US Department of Transportation office of Freight Management and Operations:

1- RFID Seals

RFID technologies are most common among electronic seals. Fundamentally, they marry RFID transponders or their components with manual seal components. There are two main types of RFID tags and seals, passive and active.

- Passive seals do not initiate transmissions—they respond only when prompted by the device used by a reader. A passive seal can identify itself by reporting its ID similar to a standard bar code. The tag can also perform processes, such as testing the integrity of a seal. A battery-free passive seal is simple, inexpensive, and disposable. Passive seals tend to be short range and directional to maximize antenna exposure to reader signal strength. Maximum read range for electronic seals without battery-assisted communications tends to be two-three meters, with some debate in the industry about efficacy beyond two meters.
- Active seals can initiate transmissions as well as respond to interrogation. All active tags and seals require on-board power, which generally means a battery. A major attraction of active tags and seals is the potential for longer-range and Omni directional communications—up to 100 meters. Expressed user needs for greater range and the ability of signals to wrap around obstructions in terminal operating environments prompted the international standards group working on electronic seal and read/write container RFID standards to add active RFID protocol(s).

Theoretically, the only difference between passive and active tags and seals is the ability to initiate communications from the tag—a distinction that means passive RFID tags could not initiate mayday calls. However, a designer could add on-board power to a passive tag, match other functionality and, setting aside regulatory, safety, and cost issues, increase read range and directional flexibility by increasing power and adding antennas. This perspective seems most appropriate to laboratory R&D discussions.

2-Infrared Seals

IR is a less common choice than RFID. It does not appear to be any standards issues about IR, but there are unresolved disagreements about its technical merits. Reported industry concerns include short range, slow data rates, effects of fog and rain, and susceptibility of some designs to generate false positive tampering signals. In addition, infrared systems are directional, offering line-of-sight performance without an ability to wrap around corners.

3-Contact Seals

These seals work in most harsh weather environments. Contact and near-contact technologies include contact memory buttons, PDA and electronic key plug-ins, low frequency RFID, and short range IR. Proponents of contact and near-contact solutions argue that it is important to have a human being visually observe the seal, and their solutions provide that added benefit. Proponents of longer-range solutions criticize the missed opportunity for labor and process timesaving.

4-Remote Reporting Seals

Remote reporting uses satellite or cellular communications. The great advantage is the ability to maintain visibility en route and to obtain near real-time event reports. It is a high-end capability, usually at high cost. As costs drop, it will become increasingly attractive for security and management applications, especially for high-value and hazardous cargo.

Box 3-1 Comparison of E-seal technologies

Type	Pros	Cons
RFID	Broad array of capabilities Passive can be very low cost Active can be high capability and moderate cost	Lack of standards, but this is being addressed Lack of global frequencies, especially in regard to active RFID
IR	Clearly effective at short ranges	Lack of clarity on strengths and shortcomings— contradictory information
Contact	Some are highly reliable in harsh environments	Contact "keys" subject to loss and misuse
Remote	Potential for immediate identification of problems Potential global coverage	High cost Usually requires significant outbound power
All	Potential to improve efficiency along with security Source: US Department of Transportation	Risks of increasing complexity, opening new avenues of attack, and generating false confidence Need for independent assessment of vendor claims Need to assess operational impacts as well as technical performance Requirement to manage and sift increased data flow, identify false positives, and act on true positives

How do they work?

Before its installation on the container the e-seal must be programmed with a handheld device by validating the container number, container type and eventually the content. The RFID bolt seal is then read at each check point using the same readers as the Container tag.

Once the RFID is installed on the container and the data is loaded it will signify if the door has been tampered with.

E-seal standards

For e-seals to be effective in helping to secure international trade, they must be useable throughout the global container transport system. This means that any e-seal affixed to a container must be readable in any transport node equipped with e-seal readers, and, conversely, reading/scanning equipment in any transport node worldwide should be capable of reading any e-seal passing through. This is not the case today as many competing vendors have proposed numerous and sometimes incompatible systems. However, many administrations and the trading community in general now agree that broadly accepted standards are necessary if e-seals are going to be effectively deployed throughout the supply chain. At a minimum, these standards should separate proprietary hardware solutions from information transmission protocols and codes.

3.3.3 Conclusion: seals

Ensuring container integrity is fundamental to ensuring container security. However, past experience with anti-theft devices and container door/handle seals have revealed the inadequacy of these devices to fully protect containers from and/or reveal unauthorized access by determined criminals. Clearly, better seals must be deployed if the container is to be targeted by terrorists. However, it would be incorrect to believe that a technological fix in the form of an advanced mechanical or electronic seal alone would be sufficient to ensure that containers are not tampered with during their voyages. Any container seal is only as good as the container stuffing and sealing process in which it is involved. This process must include controlled stuffing procedures by the shipper, seal identification and management throughout the seal's lifespan (and not just during the container voyage).

Distinction should be made between the data recorded and managed by an e-seal system that has particular security relevance such as seal status and container number, and the data that could potentially be recorded and managed by e-seal systems that have more utility from a supply chain management perspective.

Adoption of RFID in supply chain and security applications is hampered by a lack of standards and by what some call "the frequency wars." The two issues are interrelated. RFID has no global protocols or standards. For instance, RFID on which the data ride in the US will not work anywhere else. In short, RFID for container security is applicable only to those areas of the world that have agreed on the same frequency. Therefore, only a combination of RFID and satellite communication integrally linked to a human agent provides both security and logistics value in a global supply chain, and by its nature becomes the "smart container." The technologies that would make the container smart are RFID, satellite, and cellular.

However, there is still a long way to go before the "smart container" can be considered a candidate for generalized use in the supply chain. To start with, the question of specifications and interoperability needs to be solved:

"Specifications must address issues such as:

- what specifically the device would be required to do and its security value
- what acceptable false positive and false negative reading rates would be
- what radio frequency would be used
- the requirements for the installation and operation of the necessary device reader infrastructure
- the requirements applicable to the necessary communications interface and protocols with Customs
- the security vulnerabilities of such devices
- the necessity of interoperability of various vendors' devices and systems
- the data to be captured and transmitted by the device
- identification of who will have access to the data in the device
- survivability and vulnerability of the device
- power or battery life requirements
- the probability that the device can be detected, or removed without detection
- required data messaging formats, event logs, and data encryption." [36]

3.4 SCS Technologies for Container Integrity: Track/Trace or Positioning technologies

It seems evident that if authorities are concerned about the potential misuse of containers by criminals or terrorists, they should have the ability to track containers throughout the transport chain. This is not only important so that containers identified as risky can be found and inspected, but also so that containers that have gone missing like in the case of a hijacked container, can be identified and possibly found.

There are two ways containers can be tracked. The first involves recording the passage of containers through "choke points" in the container transport chain and managing the location data via database systems. The second involves utilizing a transponder or satellite-based system to deliver real-time data on the location of the container, cargo, or transport. This method is also highlighted in a case study conducted in the Middle East.

[36] Statement of World Shipping Council (WSC) before the House Homeland Security Appropriations Subcommittee Regarding "Container, Cargo and Supply Chain Security – Challenges and Opportunities." April 2, 2008

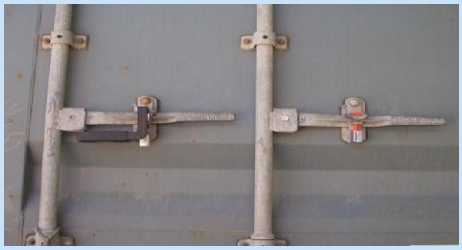
BOX 3-2 CASE STUDY ON CONTAINER INTEGRITY IN THE MIDDLE EAST

This Middle Eastern Country incorporated a transit monitoring tool for all trucks transiting through the country using a live-feed tracking software system and alarm that provides Customs officers full visibility of transiting goods aboard truck transport. This system utilizes GPS, GSM positioning and Radio technology in order to:

- Record and remotely report the location on land of every vehicle equipped with the system
- Trace all movements by the vehicle
- Detect abnormal patterns throughout the transit trip (e.g. engine status and open doors)
- Collect accurate information on specific events
- Assess risk of fraud and smuggling by analyzing information conveyed by the positioning and communication unit installed on the vehicle
- Provide adequate information to support decision making by Customs.

How Does it Work? RFID Tag and Reader with GPS

A GPS antenna is installed on the truck and an RFID e-seal is affixed onto the container. The GPS is pinging the RFID seal every 10 minutes and the data is transmitted every 20 minutes by GPS.



Most containers are tracked in the supply chain using some iteration of a "choke point" checking system. A variant of a choke point system is outlined in the case study conducted in East Africa. The checks can be accomplished manually (*e.g.* by a driver orally or otherwise confirming the loading of a particular container onto a truck) semi-automatically (*e.g.* through some form of barcode scanning) or automatically, as envisaged in several active e-seal solutions. The data generated by these checks is tracked and can be restituted with more or less ease, and more or less quickly, depending on the particular information management system in place. Container tracking within each individual system, however, can be highly effective. For instance, maritime carriers and terminal managers typically operate highly effective gate, container yard and vessel loading "choke point" tracking systems that allow them to have a precise knowledge of where containers under their responsibility can be found. However, even "low-tech" solutions can be effective. Many small road operators simply using paper and cell phone based systems can track their consignments both quickly and effectively.

The second strategy involves some form of continuous and "real-time" tracking. The main determining factor in deciding which technology option to use relates to the desired geographic scope for the tracking. The case study in East Africa highlights a low-tech choke-point tracking system.

Box 3-3 Case Study on Container Integrity in East Africa

In contrast to the technology deployed in the previous case study, the technologies used in this system are cell phones and the internet:

First, at loading, a disposable numbered seal is attributed per container. This seal number is broadcast via SMS on mobile phones to the security staff. From this point, an escort follows the transport and military style convoy techniques are applied. Along the pre-planned route, there are "visual check points" that are strategically placed at choke points to ensure there is no deviation and that the serial numbered seal matches the initial communication. Lastly, at destination the receiving agent has also received all SMS.

Basically, this SCS scheme consists of all the security layers outlined in this guide. Inspection is conducted at loading, advanced data and manifests exist via e-mail or real-time SMS feeds or voice calls, and there is physical security around the contents at all times.

In the case of relatively small areas (such as in a container terminal), real-time tracking can be accomplished via a combination of RFID tags and readers. However, real-time tracking throughout the supply chain necessarily requires some form of satellite positioning system and a related transponder. Already, several commercial solutions are available based on this principle but these are considerably more expensive than existing tracking systems.

Currently, satellite tracking is accomplished through the civilian use of the US military GPS. GPS satellites emit a weak signal that ground receivers triangulate and synchronize according to a satellite-timing signal in order to pinpoint the receiving station's location. These receivers are small and are becoming common for civilian use. Each unit, however, can cost upwards to several hundred dollars depending on its functions. While GPS is currently a widespread technology, several issues remain that should be addressed before its deployment for critical use applications – such as container tracking.

The first issue is that the civilian-use GPS signal is a degraded version of the military GPS signal. GPS systems typically integrate a software work-around to compensate for this. However, this is not so much an issue for operational GPS use anymore. The second issue is that GPS systems operate on extremely weak signals. During the cold war, the Soviet Union developed GPS-jamming and GPS emulation techniques that are now widely available in relatively inexpensive handheld devices. Depending on their power levels, they can jam or generate false GPS readings over considerable ranges. As this technology and its use are widespread, it is conceivable that a criminal organization could use an emulated GPS signal to hide its actions and deliver a GPS-tracked container to a location without raising any external alarms. Finally, GPS use in complex urban environments and in tunnels is compromised by reflected, scattered and/or unavailable satellite signals. The GPS systems are outlined below.

3.4.1 GPS

GPS is a Global Navigation Satellite System (GNSS) developed by the United States Department of Defense. It is the only fully functional GNSS in the world. GPS uses a constellation of satellites that transmit precise microwave signals that enable GPS receivers to determine their current location, the time, and their velocity (including direction).

3.4.2 GALILEO

Galileo is a global navigation satellite system currently being built by the EU and European Space Agency (ESA). The €3.4 billion project is an alternative and complementary to the US Global Positioning System (GPS) and

the Russian GLONASS. On November 30, 2007, the 27 EU transportation ministers involved reached an agreement that it should be operational by 2013.

3.4.3 GLONASS

GLONASS is a radio-based satellite navigation system, developed by the former Soviet Union and now operated for the Russian government by the Russian Space Forces. It is an alternative and complementary to the United States' GPS and the planned Galileo positioning system of the EU. Development on the GLONASS began in 1976, with a goal of global coverage by 1991.

Beginning on October 12, 1982, numerous rocket launches added satellites to the system until the constellation was completed in 1995. Following completion, the system rapidly fell into disrepair with the collapse of the Russian economy. In 2001, Russia committed to restoring the system, and in recent years, , with the Indian government as a partner, has diversified, and accelerated the program with a goal of restoring global coverage by 2009.

3.4.4 COMPASS / Beidou-2

The Compass system (also known as Beidou-2) is a Chinese project to develop an independent global satellite navigation system. Compass is not an extension to the previously deployed Beidou-1, but a new GNSS system similar in principles to GPS and Galileo. The new system will be a constellation of 35 satellites, which includes five geostationary orbit (GEO) satellites and 30 Medium Earth Orbit (MEO) satellites that will offer complete coverage of the globe.

3.4.5 Indian Regional Navigational Satellite System (IRNSS)

The Indian Regional Navigational Satellite System (IRNSS) is an autonomous regional satellite navigation system being developed by Indian Space Research Organization, which would be under total control of Indian government. The requirement of such a navigation system is driven by the fact that access to Global Navigation Satellite Systems is not guaranteed in hostile situations.

The government approved the project in May 2006, with the objective to have the system completed and implemented by 2012. It is unclear if recent agreements with the Russian government to restore their GLONASS system will supersede the IRNSS project or feed additional technical support to enable its completion.

3.4.6 Conclusion: Container Tracking

While in the end, developing some form of global multimodal “choke point” container tracking system may be desirable, presently it is probably more effective to help carriers to optimize their own tracking systems and to ensure that appropriate government agencies have access to this data as needed.

One of the key questions related to container tracking is the issue of timing. Does the container tracking system in use provide sufficiently current and useful data so that threats can be acted upon? The focus of container tracking should not necessarily be real-time data but “right-time” data. In some instances, real-time data may be appropriate and useful (as in the case of hazardous substances and/or in regions known to harbor terrorist operatives), but in many others, existing choke point tracking systems might be perfectly adapted to tracking containers. It may be sufficient to know, for instance, that a container was arriving late at a checkpoint and know who the last carrier was and how contact can be made.

After all, tracking just tells us with some certainty where the transponder is, not necessarily the vehicle itself.

Finally, countries should fully assess whether real-time tracking systems based on GPS technology are sufficiently robust at this stage for security-sensitive operations such as container tracking. At a minimum, these should not be deployed without the back up of a more traditional chokepoint control tracking system. Furthermore, given the cost of GPS-enabled transponder devices, it is not at all clear that their use should be mandated for all containerized consignments. Again, appropriate risk management exercises might better target these systems for specific uses.

3.5 Advanced Inspection Technologies (AIT)



Before inspection technologies can be further discussed, a baseline definition must be established for the three types of inspections that are commonly used when discussing the container and its contents:

1. Screening: described as the targeting and risk management process. Customs should screen information on 100 % of import containers (see ACI). Each and every container identified as high risk is subsequently scanned and, if needed, physically inspected.
2. Cargo scanning or non-intrusive inspection (NII) is a method of inspecting and identifying goods in transportation systems without a time intensive unloading process. It is often used for scanning of intermodal freight containers. NII and the physical inspection of a container's contents are conducted in order to provide Customs officials with the ability to verify the accuracy of information provided by shippers on a container's contents and the effectiveness of container integrity measures. Scanning is important because it can help identify dangerous cargo when the originating shipper, or the party responsible for stuffing and sealing the container, appears to be legitimate (AEO) but has actually been infiltrated by a criminal group. In these cases, other layers of security may provide a false sense of security because the shipments appear to be outwardly "legitimate" when in fact it is illegal.
3. Physical Inspection: Based on the results from screening and/or scanning the container is opened and unstuffed for a visual verification of contents. This generates extra-costs and delays.

Screening, scanning, and physical inspection of containers, while complementary, are not the same. 100% container screening is possible, should an administration choose to do so – 100% scanning and inspections, on the other hand, are not viable due to the backlog at Customs in ports, nor is it economically feasible for all countries. Screening can be improved with additional sensor-based or information-based inputs. Additional data, whether from the container, *i.e.* tamper indication, from the facility infrastructure, *i.e.* radiation detection portals, or from information systems, additional shipment detail, could be used to improve the screening/targeting processes.

3.5.1 *AIT Methodology and practice*

The following snapshot from case studies in East and West Africa provides insight in how screening, scanning, and inspection complement each other.

Box 3-4 AIT Case Study of AIT process of Ports in West and East Africa

Both of these countries use AIT through a Risk Management system to ensure a more efficient allocation of: Customs resources by designating the appropriate level of intervention required for each import transaction. This ranges from "Fast Track Release" (documentary check only), X-Ray scanning and then inspection through a physical examination. The following process is employed in these ports, random scans are conducted:

- Collect intelligence, e.g. manifest data to analyze anomalies and other discrepancies of container and their documentation
- Rank containers by risk, then scanning and (if needed) inspect the contents of containers as appropriate
- Employ technology (e.g., scanning devices) only in a well-crafted systems framework to minimize the impact on the flow of trade.

This risk based approach of screening and targeting for scanning has increased throughput, increased revenue, and increased security.

Generally, two types of scanning variants can be distinguished:

- Active scanning: A system making container images based on X-rays or Gamma ray beams.
- Nuclear detection: A passive system detecting nuclear and other radioactive materials based on their radiation levels

3.5.2 Nuclear detection

In September 2006, an amendment was proposed for the US SAFE port act in which Nuclear Detection will become mandatory for US-bound containerized cargo. Many of the largest ports in Europe, Asia and the US are in the process of installing radiation detection portals. Almost all these programs take place under responsibility of Customs.

Radiation Portal Monitors installed at Port of Felixstowe (UK).

However, adding to the predicament of the decision-makers, recent tests of the new generation of radiation detection portals, the Advanced Spectroscopic Portal (ASP), developed under the aegis of the US Government, have cast doubts on its ability to detect radioactive material significantly better than the existing generation. On the other hand, the estimated lifecycle cost for one of the new generation ASP exceeds US$ 800,000 or almost the triple of the cost of existing radiation scanners.[37]

While the continuous research and development of NII technologies are needed to detect hazardous cargo without interrupting the flow of goods, one technology cannot detect everything. Thus, the combination of technologies and attentive human operators is necessary. In order to justify the eventual installation of scanning devices, it can be noted that multiple benefits and objectives might result from a good scanning

[37] US GAO report 09-655 "Combating Nuclear Smuggling", June 2009

system. Improving scanning ability could serve not only to detect Nuclear or other WMD weapons but also to reduce smuggling, to improve tax collection and to earn the trade community's trust to attract more trade.

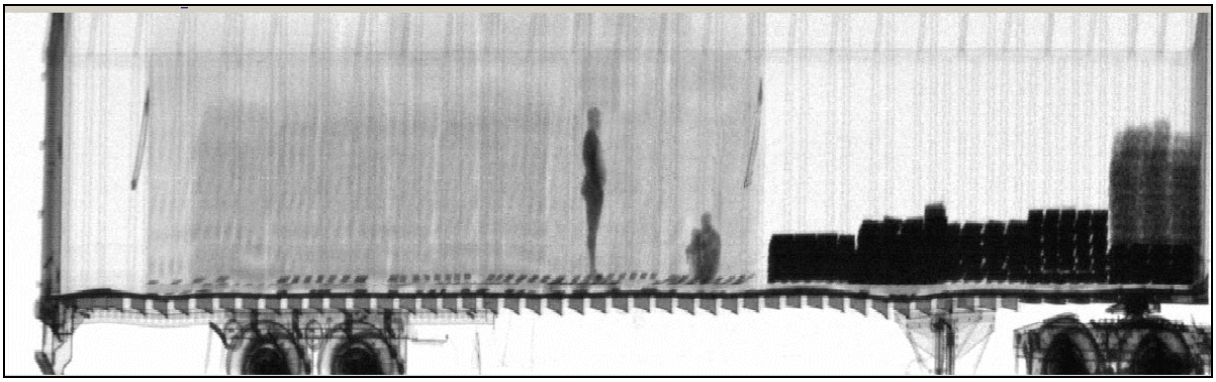
3.5.3 X-ray and Gamma-ray radiography

Advanced Inspection Technologies (AIT) first gained prominence for manifest verification, allowing countries to better enforce import tariffs. Authorities also found that the image quality achieved with X-ray scanning allowed them to interdict contraband, including drugs, cash, weapons, and other illicit materials. X-ray radiography systems can penetrate up to 30-40 cm of steel in vehicles moving with velocities up to 13 km/h. They provide higher penetration but also cost more to buy and operate. During the last few years, attention has shifted to security concerns, where X-ray screening is expected to become a major tool in prohibiting the smuggling of weapons of mass destruction. X-ray inspection systems for cargo containers have now become a more familiar feature in numerous ports. This rapid adoption has been accelerated by the needs of port security, but made practical by the systems' unique ability to penetrate entire containers and generate images of the contents in just a few seconds. Even at this large scale, the resulting images are comparable to those obtained through traditional baggage scanning at airports and capable of identifying objects smaller than a baseball.

The inspection layer also allows for Customs administrations of both the originating and importing ports to conduct inspections on the same container and can require the container to pass through different types and increasing levels of inspections. The following highlights the built-in layers of a scanning operation.

Active scanning using Gamma-ray radiography

Gamma-ray radiography is an alternative to X-ray but uses a radio-active source for the radiation.



Gamma-ray image of a truck with two stowaways in a container of Styrofoam trays entering US from Canada at Buffalo, N.Y. Image taken using 1.25 MeV photons.

As X-ray cargo scanning becomes more common at ports and border crossings, its impact on container traffic is frequently discussed. This is essentially a question of system throughput, which varies by the type of X-ray system chosen and how it is operated within a port facility. X-ray cargo screening has been adopted at ports and border crossings throughout the world because this technology has solved a number of important problems. This is where the scanning debate lies: is it for revenue or security? All stakeholders should keep in mind the fact that, while container inspections are critical from both security and revenue perspectives, efficiency (throughput) and port operations cannot afford to slow down. However, as shown in Table 3-1

Customs continues to increase the rate of discrepancies that capture revenue that would have otherwise been lost to importer error or deception. From a security stand point one can imagine what some of these discrepancies revealed.

The human side of the scanning process should also be examined so that the inspectors are well trained to interpret the x-ray images and other indicators. Experts argue that better training of Customs staff on analyzing scanned images, the digital revolution and related efficiency gains, diffusion of innovation, as well as growth and specialization in the scanning manufacturing sector will enhance security and efficiency. When analyzing the data in Table 2-1, the trends between 2001 and 2008 show an increased age in the number of proven discrepancies. With this data it becomes evident that with more training the proficiency of the operator increases, thus indirectly resulting in a more secure supply chain.

Table 3-1 Containers scanned in West Africa Port

Year	Containers Scanned	Discrepancies Proven	Percentage
2000	7,480	103	1.38
2001	13,878	542	3.91
2002	19,767	770	3.90
2003	13,563	489	3.61
2004	9,595	344	3.59
2005	13,163	803	6.10
2006	12,079	1,055	8.73
2007	13,811	1,176	8.51
2008	13,842	1,140	8.24

In contrast to the efficiency argument is the adverse effect these technologies could possibly have on developing countries. The added burden for these countries to implement systematic scanning on exports, the possibility of smaller ports being marginalized, cargo diversion in favor of hub ports, loss of expertise , such as Risk Assessment techniques and some opportunity costs are all concerns.

3.5.4 The Dual Role of Scanning

Scanning can serve two clearly distinct purposes:

- Assist in detecting and counter illegal material movements by organized crime, be it contrabandist or terrorist in nature
- Assist Customs to protect and enhance tax collection against fraud and mis-declaration by the trade or their representatives.

The two functions sometimes overlap, often through the use of the same technology, facilities and/or operating personnel.

Having one scanner in one port to inspect imports to protect or enhance tax revenue should not normally be considered as fully addressing supply chain security per se. In fact, improved monitoring of possible smuggling of weapons, explosives and similar, an important objective of SCS, is actually a collateral benefit of tax-related scanning.

There are examples of tax collection-related import cargo scanning operations in developing countries, particularly Africa. One of the implantation models is the following: a provider is granted a Build, Operate, and Transfer (BOT) concession to install and run import scanning operations. The concession often encompasses physical installations, supply and operation of one or more scanners and a risk management system, capacity building, transfer of know-how and training of the local Customs officers.

While the tax-collection improvement objectives are reportedly achieved and even exceeded in some cases, the physical insertion of the scanning procedures and sites have not always been well thought of, and the necessary consultation with the port and trade communities, as well as between concerned government agencies have sometimes been lacking. Complaints have been heard in some ports about the high costs being recouped from the logistics operators and cargo interests, as well as about the delays and interferences sometimes caused on the cargo flows and port operations. The effectiveness of the capacity building and know-how transfer components has also been questioned in some cases.

It is not the purpose of this guide to analyze in depth these tax-collection scanning schemes, but practical lessons might be drawn from these experiences.

3.5.5 Fast Scanning

One of the clear future directions of scanning is "fast scanning". Fast Scanning implies that the shipment container could be scanned while in motion at a reduced speed in the port. It is in a way similar to the automated prepaid highway toll principle. This type of scanning is already undergoing investigation by a number of major ports due to their concern in addressing the US 100% scanning requirement as discussed in this document.

There are some limitations however to fast scanning. First, as the cargo is in movement and as conveyance vehicle operators are often involved, the scanning beams have to be of relatively low power and penetration. With this type of lower penetration scan, the images do not provide the same capability to discern the container contents to the full level of detail. Second, due to this less detailed image, secondary inspections will be required on a more frequent basis in order to address this weakness.

Fast scanning is in the early stages of development – early systems include road and rail portals that are either planned for testing or currently undergoing testing by ports that are "early adopters" of technology who want to ensure their competitiveness in the current and future supply chain security environment.

In general fast scanning consists of three integrated technology elements, more specifically:

- Identification of the goods/container (RFID, optical character recognition of the container number or other similar technologies)
- X-ray scanning of the container
- Radioactive threat detection.

Once the scanning is complete the container needs to have a high security seal affixed (if not already the case), so that any tampering with the contents can be noted. And if the seal is found to be not intact at any point in the port process, a new scan will need to be done. It is also important to note that with fast scanning it is envisaged that not all images will be viewed and analyzed as there will be risk based decisions made using additional tools such as a risk management system and profiling.

Fast scanning cannot be implemented as a stand alone system as there will be requirements for secondary high penetration scans and even physical goods inspections if and when anomalies are found. Implementation of fast scanning is normally oriented solely toward outgoing shipping containers and will require re-thinking of port logistics for containers coming into the port by road and by rail. All incoming containers will need to be routed through the fast scanning systems, so this implies strictly controlled access, although in practice this has already been implemented in most ports. Many of the larger ports are already preparing for and testing

fast scanning as an early implementation measure if and when the 100% scanning requirement is implemented.

3.6 Supply Chain Security Technology Discussion/Conclusion

- Beyond the initial apparent consensus about technology – nobody wants to be seen as "anti-technology" – the heterogeneous look of this chapter is reflecting diverging opinions, angles and approaches on the issue. The debate is live, lively and ongoing, and it is the role of this guide to mirror this current situation. There are enthusiasts on the side of the technology developers, and doubters in the port and maritime industries who would end up having to deploy – and probably finance the technologies. The lawmakers are in-between with their wisdom, sagacity, pragmatism, realism and objectives.
- Research & Development should target new technologies for low-cost, high-volume remote sensing and scanning. Current sensor technologies for detecting weapons or illegal shipments are expensive and typically impose delays on the logistics system. As a result, security efforts have focused on technologies or processes for identifying containers that have been tampered with, for making it harder to tamper with containers, and for risk management purposes to reduce the burden of volume on screening containers. All these approaches have a common weakness: They are easy to circumvent. Tamper-resistant seals can be fooled, spoofed or "e-tampered". Profiling processes can be gamed as criminals learn what characteristics trigger profiling algorithms. New detection technologies for remote scanning of explosives and radiation would provide valuable capabilities for better securing the container shipping system.
- Technology development must also be coordinated with market requirements to produce devices with low development and deployment costs that contribute to attend real needs from the industry.
- Technology plays a particularly important role in providing for screening of cargo at the critical nodes of the supply chain through data acquisition, delivery, and analysis (e.g., the secure transmission of cargo manifests). The main issue in this context is a lack of capacity in the countries which most need it
- The bigger challenge is not technical but whether developing countries can apply the available technology into viable and responsive systems. This will require cooperation among domestic agencies, scenario building and high level support from finance ministries and leaders to understand that success depends on resources and political will.
- Also, the mobilizing of private sector participation in providing the ICT capacity and services required is important, and if necessary, how to finance that participation through capacity building programs.
- The private sector is already actively adopting ICT in managing their domestic and international supply chains. These developments might, with appropriate policies and international coordination, both be bolstered, through new approaches to e-government), and enhance border protection capabilities through better and more accessible information.

3.6.1 Relevance of Costs and Benefits for Developing Countries

A major issue when thinking about the formulation of a security initiative is the benefits and effects any security measure has on efficiency. An OECD study estimates that the transaction cost of inefficient trade procedures amounts to between 1 and 15 % of a products value (Walkenhorst and Yasui, 2003). This "higher

figure is more often the case in developing countries where it is complicated and costly in terms of both time and money to fulfill the requirements laid down for the import and export of goods" Kommerskollegium (2008). To compound matters, developing countries do not possess sophisticated security procedures and technology to improve efficiency. While the potential benefits of improved technologies and a coordinated approach for improved trade facilitation and security are agreed upon amongst nearly all countries, the means of getting there and who gets to determine what exactly are the current and future globally-accepted norms has created much disagreement between the EU, the United States, developing countries and their respective private sector operators.

Developing countries are generally in agreement with the benefits of trade facilitation and a coordinated approach. On the other hand, many feel that the costs associated with addressing threats to security are very high and in many cases unnecessary. They point out that an already difficult trading context exists, including inadequate infrastructure, difficult terrain and great distances between trade partners. Moreover, when added to severe budget limitations and their immense reliance on foreign trade and investments this proves to be a difficult combination. These countries therefore argue: "Why make it even more difficult for us to participate fully?"

Recent research highlights these concerns. Hummel, for example, shows that the transport costs of developing countries are on average two to four times higher than in developed countries (Hummel, 2001). In addition, the volume of goods is generally far less, meaning that ships need to call at more ports for the purpose of better capacity utilization. There are a number of difficulties that are a common feature for many developing countries:

- Frequent reloading of goods
- Overloading and bottlenecks which affect port time for feeder ships
- Complicated Customs procedures
- Complex and non-transparent requirements which often apply to documentation
- Limited use of computerization which leads to high costs for information management
- Uncertainty regarding the extent to which legal trade documents such as sea freight notes and letters of credit are valid.

Developing countries might legitimately consider that their circumstances should be taken into consideration by international governing bodies and the developed world before global standards such as AEO and 100% scanning are implemented. They suggest that the high financial costs imposed by security certifications are overburdening. However, they are caught in a vicious circle: "As more and more countries introduce certification programs for security in the supply chain there is a risk that countries that lack resources and have inefficient systems for the exchange of information and security controls will not share in the benefits proposed by these programs and even experience a deterioration in their prospects of participating in international trade".

4 CONCLUSION

SCS is a relatively new issue to developing countries within the context of international trade. One of the key messages is **"start as soon as possible"!**

This applies for both governments and the private sector. For governments, mutual recognition is the important issue to be addressed early in the process, but this first requires that a national SCS program should be in place. The complexity of the issue is significant and requires first an in-depth understanding of the components needed and the path for implementation. This document has attempted to provide both in a clear fashion.

For the private sector, logistics and supply chain operators need to address the threats to their business and their supply chain, and the requests from their partners and clients. It is possible that in the future trade partners and logistics operators who are not SCS certified will find that they are "discarded" by their usual trading partners. As more and more private sector operators become certified, the non-certified list could potentially eventually become a "going out of business" list. Non-certified operators will find themselves to be more and more in the spotlights of Customs attention, which will mean a competitive disadvantage.

The next important conclusion is that there are many tools available to assist both governments and the private sector to implement SCS. These tools are described in detail and referenced within this guide. For governments, the WCO SAFE Framework of Standards and multiple diagnostic and implementation tools are available from the World Customs Organization. These tools are discussed in depth throughout this Supply Chain Security Guide.

For the private sector, specific SCS standards, guidelines and self assessment tools exist. Key examples are the ISO 28000 series of Standards, the C-TPAT Best Practices Catalog, the C-TPAT Minimum Requirements (per trade actor), the EU AEO guidelines and the AEO Self-Assessment Checklist. In general, these guidelines and checklists are considered to be quite comprehensive in covering the necessary SCS issues.

The most visible actors involved in SCS, namely the ports and the merchant vessels, have been addressed to a large extent, by two compulsory regulatory requirements:

- The ISPS code
- The 24 Hour Advance Manifest Rule and similar ACI regulations.

The more variable components, upstream and downstream of the ports, are being addressed by voluntary certification programs (such as C-TPAT and other AEO certification programs). These programs all have a built-in network pressure effect, as each certified entity is supposed to demand compliance from its suppliers and service providers as well.

In the end, the objective is to have as many certified AEOs entities as possible, allowing Customs and enforcement authorities to focus on the uncertified players, with only random checks on the certified AEOs compliant operators.

As the container becomes a virtual mobile warehouse in support of just-in-time inventory control, various technologies and supply chain procedures must support the new business processes, new standards and new regulations that are designed to address supply chain management weaknesses. It is also important to address global criminal and safety issues such as product counterfeiting – and in fact, most supply chain

security measures have elements which also have the additional benefit of addressing these issues as well. SCS initiatives, and supply chain modernization efforts will continue to accelerate, as will the implementation of new technologies. It must be emphasized however, that the international bodies, regulators and policy makers must collaborate with the technology developers and the trade, port and transport industries in order to ensure that these new technologies can be implemented and incorporated in an economic and sustainable way by all nations engaged in trade.

There are three main issues currently requiring a sustained attention:

- Mutual Recognition of "Authorized Economic Operator" SCS certification programs
- The US 100% scanning law
- Cautious and sustainable use of emerging technology.

It is evident that many national SCS programs are being implemented or will be implemented over the coming years. This then begs the question of mutual recognition of AEO programs and the issue of the multiple SCS layers which will be encountered by the business and trade community. Finally and again to stress the point, mutual recognition is one of the key objectives for the future. National administrations will have to make efforts to address this, with the main beneficiaries being the companies that operate in multiple countries with different SCS certification programs.

As for the second issue of the US 100% scanning law, there remain many difficulties with implementing this requirement and in fact in February 2009, Secretary Napolitano of the US Department of Homeland Security (DHS), alerted the US Congress that due to logistical concerns expressed by shippers and carriers and diplomatic concerns expressed by foreign governments, it was envisaged that DHS will not meet the 2012 deadline to scan all cargo bound for US seaports.

On the other hand, there are no signs that the sponsors of this legislation will relent in any way, in spite of the international skepticism. As far as can be predicted today, the law is there to stay, and the stakeholders need to keep an eye on how a possible compromise will be reached, if any, and what the end product will look like.

Concerning the third issue, while private technology vendors might develop appealing high-tech solutions, it belongs to governments and international organizations to verify that such solutions actually do address –and solve- real problems, and that they do so in an affordable and cost-efficient manner, with due regard to their global interoperability. Technology development must also be coordinated with market requirements to produce devices with low development and deployment costs that contribute to attend real needs of the port and transport industry without disrupting their efficiency.

Great care and broad consultation must be exercised by lawmakers when pondering the sustainability of incorporating high-tech components in the SCS programs which have a global vocation. The economic viability and the institutional capacity aspects are central to the analysis of a program's affordability for all nations engaged in international trade.

The expected end vision of SCS is a global, regional and national networked and layered approach to SCS with mutual recognition of national and regional AEO programs. The layered approach necessitates the use of different detection, integrity and ACI technologies, in addition to other related regulatory and programmatic requirements. SCS programs will need to have defined benefits and incentives that can be quantified to those who wish to participate in the program. Without defined and proven benefits to the program participants it is difficult for these organizations to make the cost/benefit decision and more often than not, participants will

only consist of those forced by their trading partners or the business environment to enter into the specific SCS program (and those who can afford it).

The tools outlined and referenced in this document are intended to assist both the trade community and governments to understand the basics and initiate the first steps to implement SCS in their respective areas of jurisdiction.

5 REFERENCES

Published sources

Bhat B., Peleg-Gillai G. and Sept, L. 2006. "Innovators in Supply Chain Security: Better Security Drives Business Value." *Manufacturing Innovation Series*.

Bichou, K. 2008. "Maritime Security and Risk-based Models: Review and Critical Analysis." DiscussionPaper No. 20. Prepared for the OECD/ITF Round Table of 11-12 December on *Security, Risk Perception and Cost-Benefit Analysis.*

Bichou K. 2004. "The ISPS Code and Cost of Port Compliance an Initial Logistics and Supply Chain Framework for Port Security Assessment and Management." *Maritime Economics and Logistics, 6*.

Closs, D. and Mcgarrell, E. 2004. "Enhancing Security Throughout the Supply Chain. Special Report Series." *IBM Center for The Business of Government*.

Dayton Business Journal, November 13, 2008

Diop, A. and Hartman, D. 2007. "Customs-Trade Partnership Against Terrorism – Cost/Benefit Survey." Paper prepared for the US *Customs and Border Protection* Agency.

ECMT and OECD Maritime Transport Committee Secretariats. 2004. "Task Force on Security and Terrorism in Transport." Prepared for the *European Conference of Ministers of Transport* on 5 March.

Erera A., Kwek K., Goswami N., White C. and Zhang H. 2003. *Cost of Security for Cargo Transport*. The Logistics Institute.

eyefortransport. 2005. "Cargo and Supply Chain Security trends." eyefortransport *Cargo & Supply Chain Security Report*.

Florida Shipper. 2007. "Scan-all fallout: Lines might refuse US imports." August 27.

Gutiérrez X., Hintsa J., Wieser P., and Hameri A.P., 2007. "Voluntary Supply Chain Security Program Impacts: an Empirical Study with BASC Member Companies. Vol. 1, No. 2. *World Customs Journal*, Brussels.

Gutiérrez X. and Hintsa J. 2006. "Voluntary Supply Chain Security Programs: A Systematic Comparison." Paper prepared for *the International Conference on Information Systems, Logistics and Supply Chain*. Lyon, France.

Hintsa J., Gutiérrez X., Hameri AP., and Wieser P. 2009. "Supply Chain Security Management: an overview." *International Journal of Logistics Systems and Management*, Vol. 5, Nos. 3/4.

Hintsa J., Hameri AP., and Tsikolenko V. 2005. "Impacts of New Supply Chain Security Regulations and Programs in International Trade and Cross-border Operations Automation Systems – A Preliminary Study." Paper presented at *The First International Conference on Transportation Logistics*, Singapore, 27-29 July.

Hummels, D. 2001. *Time as a trade barrier*. Purdue University, West Lafayette.

Kommerskollegium. 2008. *Supply Chain Security Initiatives: A Trade Facilitation Perspective*. The National Board of Trade, Sweden.

Kruk, C., Donner, M. 2008. "Review of cost of compliance with the new international freight transport security requirements", The World Bank, Washington, D.C.

Lee, H. and Wolfe, M. 2003. "Supply Chain Security without Tears." *Supply Chain Management Review*, Vol. 7, No. 1.

Mikuriya, K. 2007. "Supply Chain Security: the Customs Community Response." *World Customs Journal*, Vol. 1 No. 2.

Miller, John. 2007. "New Shipping Law Makes Big Waves In Foreign Ports." *Wall Street Journal*, October 25.

Monahan S., Laudicina P. and Attis D. 2003. "Supply Chains in a Vulnerable, Volatile World." A.T. Kearney Executive Agenda, Vol. 6 No.3.

Organisation for Economic Co-operation and Development, and European Conference of Ministers of Transport. 2005. Container transport security across modes. Paris: OECD.

Rice, J. and Caniato, F. 2003. "Building a secure and resilient supply network." *Supply Chain Management Review*, Vol. 7, No. 5.

Rice, J. B. and Spayd, P. W. 2005. "Investing in Supply Chain Security: Collateral Benefits." *Special Report Series, IBM Center for The Business of Government*.

Sarathy, R. 2006. "Security and the Global Supply Chain." *Transportation Journal*. Vol. 45, No. 4.

University of Le Havre/WCO, Global Logistic Chain security, Economic impact of the US 100% scanning law, June 2008.

US AID. *International Supply Chain Security and its impact of Developing Countries*. Washington.

Walkenhorst P and Yasui T. 2003. *Quantitative Assessment of the Benefits of Trade Facilitation*. OECD, Paris.

WCO News. 2008a. "Safe Versus 100% scanning: Interview with Michael Schmitz." No. 55. Brussels.

WCO News. 2008b. "100% scanning: The European Union strategy." No. 55 Brussels.

World Customs Organization, 2008. *Professional standards*. Brussels.

Widdowson, David. 2007. "The Role of Capacity Building in Achieving Consistent Application of International Standards." *World Customs Journal* Vol. 2, No. 2. Brussels.

Web documents and websites

Australia Customs Service. http://www.customs.gov.au/site/page.cfm

Business Alliance for Secure Commerce. http://www.wbasco.org

Business Alliance for Secure Commerce, *What is BASC?* http://www.wbasco.org/english/history.htm

Canada Border Services Agency. http://www.cbsa-asfc.gc.ca/menu-eng.html

C-TPAT -Customs-Trade Partnership Against Terrorism http://www.geosbush.com/ctpat.html

European Commission Taxation and Customs Union. *Pre-arrival Pre-departure* http://ec.europa.eu/taxation_Customs/customsCustoms/procedural_aspects/general/prearrival_predeparture/index_en.html

Federal Highway Administration. Freight Management and Operations. http://ops.fhwa.dot.gov/freight/publications/eseal_wp_final_july12/eseal_wp_final_04.htm

ISO28000. 2005. *Specification for Security Management Systems for the Supply Chain*. http://www.iso.org/iso/catalogue_detail?csnumber=41921

International Maritime Organization. *FAQ on ISPS Code and Maritime Security*. http://www.imo.org/Newsroom/mainframe.asp?topic_id=897

International Maritime Organization. *FAQ on ISPS Code and Maritime Security*. http://www.imo.org/Newsroom/mainframe.asp?topic_id=897

Intermodal Freight Technology Overviewtime Organization (http://ops.fhwa.dot.gov/freight/intermodal/ift_overview.

Japan Customs. http://www.customs.go.jp/english/

Labuda, J. 2000. *Risk Management and You*. US Customs Today, December http://www.cbp.gov/custoday/dec2000/risk.html.

New Zealand Customs http://www.customs.govt.nz/default.htm

New Zealand Customs Services, *Fact Sheet 34 – Secure Export Scheme*. http://www.customs.govt.nz/NR/exeres/3A21F54F-D9E1-4E7A-8386-327924194743,frameless.htm?NRMODE=Published

Sigma. 2008. *Natural catastrophes and man-made disasters*. http://shequ2.tool.hexun.com/ExpertFiles/20080409/363810/F9579F9BD58D1773D30999ADE1C96211.pdf

Singapore Customs http://www.customs.gov.sg/topNav/hom/html

Singapore Customs. Secure Trade Partnership. http://www.customs.gov.sg/leftNav/trad/Supply+Chain+Security.html

Supply Chain Council http://www.supply-chain.org/

US Customs and Border Protection. http://www.cbp.gov/

US Customs and Border Protection. 2004. *Securing the Global Supply Chain, Customs-Trade*

Partnership Against Terrorism (C-TPAT) Strategic Plan http://www.housewares.org/pdf/iha/global/CTPATStrategicPlan.pdf

US Customs and Border Protection. *Secure Freight Scanning at a Glance*.¨
http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/trade_security/sfi/sfi_scanning.ctt/sfi_scanning.pdf

US Government Accountability Office http://www.gao.gov/

World Customs Organization. http://www.wcoomd.org/home.htm

World Customs Organization, *Programs*. Brussels.
http://www.wcoomd.org/home_wco_topics_cboverviewboxes_programmes_cbcolumbusprogrammeoverview.htm

World Customs Organization. 2005. *Self-Assessment Checklist, Framework of Standards to Secure Safe Trade*. Brussels.
http://www.wcoomd.org/files/1.%20Public%20files/Images/Publications/OMD_News_58_UK_MEDIUM.pdf

World Customs Organization, 2005. *Framework of standards to secure and facilitate global trade, SAFE*, Brussels.http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/SAFE

World Economic Forum. 2009. *Global risks landscape*. Geneva.
http://www.weforum.org/pdf/globalrisk/2009.pdf

World Shipping Council http://www.worldshipping.org/

Interviews

Lars Karlsson, Capacity Building Director; and Henk van Zandwijk, Regional Expert, WCO, joint phone interview, 8.1.2009

DG of Royal Malaysian Customs, with 8 other RMC experts, several phone interviews, 2.1-10.1.2009

NN, Senior Manager, Port-X, the Dominican Republic, several phone interviews, 23-30.12.2008 (person name and company name are confidential)

Victor Fernandez, Senior Manager, DOW, Colombia, phone interview, 26.1.2009

6 INDEX

ANNEX I Frequently Asked Questions

- *WHAT IS SCS?*

The term "supply chain security" can be defined as a concept which encompasses the programs, systems, procedures, technology and solutions applied to address threats to the supply chain and the related threats to the economic, social and physical well-being of citizens and organized society.

There are many different threats to the supply chain which fall primarily into the categories of criminal activities and terrorist threats. The discussion of natural disasters and "acts of God" will be limited in this document, however it must be noted that many of the preventative, mitigating and recovery measures noted here are most relevant for those issues as well.

Criminal activities are by far the most important problem in international trade and transport. The criminal threats cover a wide range of aspects:

- Cargo theft
- Conveyance vehicle theft
- Goods and human smuggling
- Tax and duty evasion
- Attack on a transportation node.

The terrorist threats to SCS can be categorized as follows:

- Use of the cargo as a weapon
- Use of the container as a weapon
- Use of the container as a delivery mechanism or to move weapons, explosive, biological and radiological contaminants and their precursors
- Use of the conveyance vehicle as a weapon
- Use of the conveyance vehicle as a delivery mechanism
- Industrial espionage, sabotage.

With the goal of the terrorist activities being:

- Damage, destroy, or exploit the supply chain, logistics systems, infrastructure and information management systems
- Cause victims and casualties
- Cause economic harm and cost
- Results of reduced freedoms and loss of the feeling of well-being.

In order to effectively counter these threats and their consequences there are 5 key pillars to SCS, these are:

- **Awareness**: identify / understand threats, assess vulnerabilities, determine potential impacts and consequences
- **Prevention**: detect, deter and mitigate threats
- **Protection**: safeguard people, critical infrastructure, property from criminal acts
- **Response**: manage and coordinate the response to criminal acts or other emergencies

- **Recovery**: manage efforts to restore operations after criminal acts or other emergencies.

Who are the principal players in SCS?

The table below describes the supply chain participation roles of the principal players in SCS.

Table I-1 Participation roles of main players in SCS

Role	Supply chain participants
	Third Party Logistics Provider (3PL)
	Buyer (consignee, importer)
Transaction Facilitation	Buying Agent
	Freight Forwarder or NVOCC
	Customs Broker
	Ship's Agent
Transport Task (physical movement of cargo / container)	Empty Container Depot Operator
	Warehouse/Container Freight Station Operator
	Multi-modal Terminal Operator (e.g. road-rail, road-barge, rail-barge)
	Trucker/Intermodal freight transport (short-haul, long-haul)
	Rail Carrier
	Barge Operator
	Ocean Carrier
	Port Terminal Operator
	Other Port Service Operators
Authorizing/ regulatory	Customs & Immigration Authority
	Import/Export Licensing Authority
	Agriculture, Sanitary, and Veterinary Authority
	Port Authority
	Import/Export Statistical Agency
	Others (Chambers of Commerce, Consulates, etc.)
Financing	Banks (Seller's or Advising Bank, Buyer's or Issuing bank)
	Insurance Provider (Carriage Insurance)

Why is it important to know about SCS?

Many governments and many players in the private sector may ask the question: "How does SCS affect me?" The answer is different for these groups.

For the governments, the majority has signed the World Customs Organization (WCO) SAFE Framework of Standards (FoS) which requires the implementation of a national supply chain security program, which includes elements such as technology, certification and mutual recognition thereof, risk management and Advance Cargo Information (ACI). This implies that most governments are committed to develop their own national program. Thus, for WCO signatory governments it is key to understand the pillars and requirements of the WCO SAFE FoS and to start making the necessary plans to implement a national SCS program.

The WCO offers many tools to accomplish this and we point to these tools throughout this document as references.

After the implementation of a national SCS program, mutual recognition with other existing programs is the next "hot" issue. This requires a political effort on the part of the national bodies concerned and is often a matter of time and especially trust in the nation-to-nation relationship. Mutual recognition is discussed in this

document as one of the as yet unresolved issues since only few states have signed agreements mutually recognizing the national supply chain security certification of one another. Despite such problems, there is however no need to reinvent the wheel, since, for example, the WCO SAFE Framework of Standards' (WCO SAFE FoS) proposed tools offer an internationally, thus multilateral, accepted platform, which will help to facilitate downstream mutual compatibility and recognition – if adequately implemented.

For the private sector the motivations are different. Competitive forces, industry demands, and an increasing number of incidents such as theft, piracy and natural disasters at outsourced locations have all caused a spike in the awareness level of security. This is especially true in the area of risk management. Today the business case for investing in security is focused on two areas: 1) business continuity in the event of a catastrophe or other disruptive event causing a discontinuity in business operations and 2) the reduction of theft/crime. It is also important that the private sector weighs the costs against the benefits of participating or not in the various national and international programs, which will be discussed in Chapter 1 of this guide.

For the private sector, more and more it is becoming: "If you are not "in", you are "out" ", meaning that although SCS programs are voluntary in most cases, if you are not participating, the company runs the risk of being left out of the international trade and transport process or may find itself at a competitive disadvantage compared to competitors who are "in".

As to the private sector, there are two main programs: the US Customs-Trade Partnership Against Terrorism (C-TPAT) and the European Union Authorized Economic Operator (EU AEO). There are many other national, regional and private sector led programs and these are described in detail in Chapter 1.

What is Supply Chain Security Management (SCSM)?

According to Hintsa (2009), SCSM covers all processes, technologies and resources exploited in a systematic way to fight against end-to-end supply chain crime. The primary goal of each single SCSM measure is either to prevent a crime, to detect a crime, or to recover from a crime incident in the fastest possible time. Single SCSM measures fall typically into one of the following five categories: cargo, facility, human resources, information technology, and management systems. The typical supply chain crime includes theft, smuggling, counterfeit, sabotage for financial gain, terrorism for destruction, and any type of fraud and corruption (the detailed crime definitions subject to national and international regulations).

SCSM can be defined as the application of policies, procedures, and technology to protect supply chain assets from theft, damage, or terrorism and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain (Closs & McGarrel, 2004).

What is Risk Management?

Risk management focuses on identifying and implementing measures to limit exposure to risk, or the likelihood of an event occurring with a negative or unwanted outcome. In trade, the focus of risk management is to systematically identify imports and exports that represent the greatest risk of noncompliance with Customs laws and regulations, and the greatest risk to national security and safety. By using multiple risk management strategies in a layered approach Customs authorities can identify and target those areas that pose the greatest risk, and allocate resources accordingly. Cargo security programs generally implement similar risk management strategies based on the following: collecting data elements and detailed shipment information from a variety of sources; analyzing and assessing risk using rules-based computer programs and Customs targeting teams; prescribing action, such as undertaking non-intrusive or physical inspection or seizure; and tracking and monitoring the risk management process and its outcomes (Laduba 2005).

What is a Layered Approach?

The assumption behind the layered approach to supply chain security is that by having two or more security layers one can achieve "better security outcomes", than by investing the same amount of money into just one layer. There are numerous factors, outlined in Chapter 4, that threaten the global supply chain and therefore make it difficult in securing it. Compromised security at any node or transport link in the supply chain can prejudice the entire chain. Hence, attempts to secure the supply chain have relied on the concept of layered security. Such an approach builds redundancy and additional protection measures into the system, so that security breaches at one level can be addressed in a subsequent level. For example, in practical terms, a layered approach could consist of a combination of the following: 1) an Advance Cargo Information (ACI) regulatory requirement, 2) Implementation of risk management approach, 3) Preferable use of NII equipment, 4) Authorized Economic Operator program (a “trusted economic operator” certification program). With multiple layers of supply chain security, each layer addresses the potential weaknesses of the other implemented layers thus ensuring that the combination of elements will ensure security in a much better way than any layer on its own.

What is Mutual Recognition?

Mutual recognition is the acceptance of common security parameters and the acceptance of that certification by various countries. Currently the US C-TPAT program shares mutual recognition with the countries of Jordan, New Zealand and Canada. The US Customs and Border Protection and the European Union have already developed a mutual recognition roadmap that envisages achieving mutual recognition of the C-TPAT Program and the EU AEO program before the end of 2009.

What is the role of the Port/Cargo community?

The Port/Cargo community is one of the most important key players in supply chain security. This is both in terms of the fact that these represent nodal points in the supply chain and that relevant cargo data is captured and disseminated via systems used specifically by these players that are in this community. Evidence of their importance is demonstrated by the early adoption and implementation of the International Ship and Port Facility (ISPS) Code, even before other global measures were undertaken.

It is relevant that the port/cargo community is often one of the early adopters as they implement new measures in order to gain a competitive edge in a sector where the competition is fierce, especially when there is a difficult economic climate.

Inevitably, although these players are among the most significant, all international trade players are important in SCS as it is clear that the chain is only as strong as its weakest link.

What is the current situation of Supply Chain Security?

Supply chain crime and SCS are not new phenomena. There is a long history of crime and security. Pirates, bandits and smugglers have always affected our trade routes while the private and public sectors have always argued over what type of security should be implemented, how much security is needed, and most importantly, who should pay for the security.

The role of government agencies traditionally has focused more on issues with respect to revenue collection and protection, especially Customs for border crossings; major theft investigation, especially police; pirated products, Customs and police, and traditionally nations have set only a few binding regulations, mainly regarding dangerous goods transport and storage, and aviation. Today there are numerous SCS programs or schemes that are being set into motion by multiple sectors, often without collaboration. Differences in schemes and objectives between governments and businesses, different government offices or ministries, different countries, and different continents, will all require the involvement of the international community in order to piece together a collaborative standard. An example of a collaborative standard is outlined in the WCO SAFE Framework of Standards. While this guide will not promote any scheme over another, Chapter 2 will at least provide an analytic view on the benefits and/or the consequences of each program.

How did Supply Chain Security Management (SCSM) evolve?

Supply chain crime, as piracy, can be traced back over 3,000 years. The earliest documented act of piracy was pioneered by a group called “The Sea Peoples”. These seafaring raiders lived around 1200 B.C. and sailed to the eastern shores of the Mediterranean, causing political unrest, and disruption in all trade. Not much has changed, as we can observe today along the Eastern shores of Africa.

The terrorist attacks of 9/11 have become a defining moment for SCSM. Until then, the focus of governments was on trade facilitation, tax compliance, and the harmonization of trade rules and practices as a result of the climate imposed by the Kyoto Convention. After 9/11, global trade has experienced an extreme change in the current paradigm from facilitation and harmonization to security and anti-terrorist measures. This drastic change has modified the approach to the overall SCS discipline.

Prior to Sept. 11, 2001, most discussions of freight transportation security focused on controlling theft and reducing contrabands such as drugs, illegal immigrants, and the export of stolen cars and construction equipment. After Sept. 11, the highest-order definition of freight security changed from theft-proof to tamperproof *(Lee & Wolfe, 2003).*

Some elements of this new focus are:

- Not allowing any biological or chemical agent to be introduced to the product
- Not allowing any illegal commodity to be intermingled with the shipment
- Not allowing the replacement of the product with an illegal commodity or person
- Not allowing the shipment to be used as a weapon. (Rice & Caniato, 2003).

This new security oriented approach toward anti-terrorism also implied new requirements in supply chain management. The perception of security as limited to “inside the company” has been expanded to the entire

supply chain. A country or regional specific focus approach has been expanded to a global focus due to the interdependencies of world trade.

The 9/11 attacks dramatically illustrated the interdependence that exists in the supply network not just among the trading partners, but also with the government agencies involved in the flow of goods and the transportation infrastructure. Today's operating environment also calls for new organizational capabilities. Specifically companies will need to forge new relationships with those government agencies that are now working to make supply networks more secure. Similarly, deeper relationships need to be developed with suppliers and customers to co-create a more secure network. Internally, the biggest organizational challenge may be to give individuals a solid understanding of the interdependencies and operational imperatives that now exist (Rice & Caniato, 2003).

As a result of these new security requirements and government-business interdependency needs, security initiatives have been launched by governments, international organizations and sometimes associations, including the following:

- 24 hour manifest rule
- C-TPAT,
- Container Security Initiative (CSI) in the USA
- Business Alliance for Secure Commerce (BASC) in Latin America
- Authorized Economic Operator (AEO) program
- WCO SAFE Framework of Standards (WCO)
- Transported Asset Protection Association (TAPA)
- International Ship and Port Facility Security (ISPS) Code at a global level.

The common denominator in all these initiatives is the objective of minimizing the risk of any disruption in the supply chain, while facilitating the seamless flow of trade goods globally.

What is compulsory today?

At the time of writing, there are only 8 live compulsory SCS programs implemented in the world:

- The ACI "24 hour manifest rule" to USA (2003)
- The ACI rules to Japan, Canada and Mexico (2007)
- The ACI 10+2 rule (2009-10) to USA
- The Pre-arrival and Pre-departure ACI rule (EU) (2009-2011)
- The ACI rules to China (2009)
- The ISPS Code (2004)

The 100% scanning rule, by US law, will be implemented as from 2012.

The guide will also review what will become compulsory and when, and what is voluntary but has a good chance to become generalized practice (perhaps in a way that will resemble the spread of the ISO certification over the last decade).

What is the role of Advance Cargo Information (ACI)?

Beyond the ISPS Code, the only other compulsory SCS components hinge on Advance Cargo Information (ACI). The information is provided by all the actors in the supply chain, to allow Customs authorities to make

informed targeting and intervention decisions with dedication of resources to the high risk issues and cargoes. The ACI requirement is one of the cornerstones in any SCS program with the most relevant examples being the US 24-hour manifest rule, the US 10+2 requirement and the EU, China and Mexico.

What is required when a SCS initiative becomes compulsory?

First and foremost, many ports have already implemented the ISPS Code which goes a long way in explaining the basics of SCS. In general, SCS programs are voluntary and not compulsory, but as more and more ports and logistics operators enter the programs and initiatives, there are less and less "outsiders" who will therefore be subject to more intense controls and treatment. Thus, if an organization does not become SCS certified and the rest of the competitors do get certified, this organization will be the one that is systematically controlled. In addition, the trade partners will "deselect" the uncertified partners. This implies that voluntary adherence eventually becomes a standard practice and a necessary requirement if an entity wants to stay in business as part of the international trade supply chain.

A good parallel example to this is the prevalence, nowadays, of the requirement in many contracts for companies to be ISO 9001 certified in order to do business with certain clients. In fact, many retailers in the US and Europe are already requesting SCS certification from their trade and logistics partners and suppliers as a necessity in order to continue to be considered at all to do business with them.

What is the status of SCS from a regulatory point of view?

Programs have been implemented in quite a number of countries globally, the most notable two being the US C-TPAT program and the EU AEO. In addition, one of the most high profile and most controversial laws is the US SAFE Ports Act which requires 100 % container scanning at origin for all cargo destined for the US by the year 2012.

A most important "regulatory" model instrument (with the term "regulatory" used loosely) is the WCO SAFE Framework. As this has been signed by an overwhelming majority of the WCO members, in fact, this Framework represents the best consensus basis for a global SCS approach.

ANNEX II Glossary

100% Scanning	2007 US law that requires 100% scanning of all containers destined for the USA by the year 2012
24 Hour Rule	International security program originated from the US requiring upload of cargo data 24 hours before loading on the ship
3PL	Third Party Logistics
ACI	Advance Cargo Information, also called International Supply Chain Management (ISCM)
AIS	Automated Identification System
AEO	Authorized Economic Operator. The AEO is considered to be a party involved in the international movement of goods, who has to be approved by the national Customs administration as complying with national supply chain security standards. After having been approved (or certified), the party will receive certain benefits in terms of facilitated clearance and/or security inspections
AEOC	AEO Customs simplifications
AEOF	AEO Customs simplifications / security and safety
AEOS	AEO Security and safety
AIT	Advanced Inspection Technology (e.g. x-ray or radiation detection scanners) Similar to NII
APAC	Asia Pacific geographic region
APEC	Asia-Pacific Economic Cooperation. An economic forum for countries around the Pacific Ocean, including Australia, Brunei, Chile, Philippines, Hong Kong, Indonesia, Japan, Canada, China, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Russia, Singapore, South Korea, Thailand, USA and Vietnam
ASEAN	Association of Southeast Asian Nations
ATS	Automated Targeting System. US Customs and Border Protection targeting system which is part of the electronic customs environment
BASC	Business Alliance for Secure Commerce. A private sector security initiative in Latin America
B/L	Bill of Lading is a document issued by a carrier specifying that certain goods have been received on board as cargo for movement to a named location for delivery to the consignee

Cargo	1. Goods transported or to be transported, all goods carried on a ship covered by a B/L. 2. Any goods, wares, merchandise, and articles of every kind whatsoever carried on a ship, other than mail, ship's stores, ship's spare parts, ship's equipment, stowage material, crew's effects and passengers' accompanied baggage
CBP	Customs and Border Protection (US). The US customs authority which is an agency under the Department of Homeland Security
CCTV	Closed-circuit television. A surveillance TV system
CEDEX	Container Equipment Data Exchange
CEN	European Committee for Standardization
CIS	Container Integrity Systems
Collaboration	The act of working together to improve business processes
CRM	Customer Relationship Management
CSD	Container Security Devices
CSI	Container Security Initiative. A legal initiative in the USA which, among other things, introduced a network of security-certified ports outside the USA, with American customs personnel stationed at the ports
CSP	Customs Security Program. The name given to the EU's rules for AEO and for advance notification. It also includes common control standards, risk indicators and increased cooperation between customs authorities and other authorities inside and outside the EU member states
C-TPAT	Customs-Trade Partnership Against Terrorism (US). The CBP's certification program which is directed towards companies in the supply chain. The companies are certified from the security perspective and are given advantages in customs procedures and security-related controls
CTS	Container Tracking Systems
Defense in depth	The practice of layering defenses or placing multiple barriers between an organization's critical assets and a disruption to provide added protection
Deterrence	The ability to discourage or prevent a disruption to the supply chain
DG TAXUD	European Commission Directorate General Taxation and Customs Union
DHS	Department of Homeland Security (US)
DOE	Department of Energy
DOT	Department of Transportation (US)

EC	European Commission
E-Customs	Electronic Customs (or e-Customs) aims to replace paper format Customs procedures with electronic procedures, thus creating a more efficient and modern customs environment
E-Government	E-Government refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government[38]
EMEA	Europe, the Middle East and Africa
ETSI	European Telecommunications Standards Institute
EU	European Union
EU-AEO	International security program originating in the EU
FAQs	Frequently Asked Questions
FSR	Freight Suppliers Minimum Security Requirements. An initiative that was introduced when TAPA was established. FSR are requirements placed on general security in the supply chain and which include, for example, perimeter security, premises and security routines
GALILEO	A global navigation satellite system currently being built by the European Union (EU) and European Space Agency (ESA)
GAO	U.S.Government Accountability Office
GNSS	Global Navigation Satellite System
Golden List	International security program originating in Jordan
GPS	Global Positioning System
Green Lane	A procedure that gives certified companies free customs passage apart from random controls
GSM	Global System for Mobile Communication
ICAO	International Civil Aviation Organization
ICT	Information and Communication Technology
IIC	Intermodal Interface Center
IMF	International Monetary Fund

[38] http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTEGOVERNMENT/0,,contentMDK:20507153~menuPK:702592~pagePK:148956~piPK:216618~theSitePK:702586,00.html

Inspecting	Signifies manual inspection of containers using either X-ray or gamma ray technology or through physical inspection of the container. (Note: CBP's definition of screening can also mean "Inspecting" as defined here or the screening of information; see definition of screening below.)
IMO	International Maritime Organization. A UN agency that has drawn up security rules for shipping, the ISPS Code
IOs	International Organizations
IOS	International Information Systems
ISCM	International Supply Chain Management
ISO	International Organization for Standardization. Develops standards for ways in which the work and management of company processes linked to security should proceed
ISO 28000	International security program originated from ISO Technical Committee
ISO/PAS	International Standards Organization Publicly Available Specifications
ISPS	International Ship and Port Facility Security Code. ISPS-Code. International rules for shipping drawn up by the IMO which contain both mandatory legislation and recommendations
IT	Information Technology
ICT	Information, communication technologies
JIT	Just–in–time production Goods that are transported in a carefully calculated way to arrive at the very moment they are needed in production
JCCC	EU-China Customs Cooperation Committee
Logistics chain	All successive links involved in the logistic process
LRIT	Long-range Identification and tracking
NII	Non-Intrusive Inspection. Controls of radioactivity or inspections using X-ray or gamma-ray technology. (similar to AIT)
NVOCC	Non-Vessel Operating Common Carrier. The designation of a carrier that does not normally engage in maritime transport but which is hired by a shipping company, and becomes its partner, with the same rights and obligations as the shipping company
OECD	Organization for Economic Co-operation and Development
OEM	Original Equipment Manufacturer

OSC Operation Safe Commerce (US). An American initiative that was started with the aim of providing support to company-initiated research projects to enhance security in the international supply chain

Preparedness A state of being prepared for action

Program Unless explicitly computer related, the word **program** in this guide is understood as being a complex (a whole composed of interconnected or interwoven related parts) of integrated and sequenced methods, procedures, systems, rules, and regulations applied to segments or components of the supply chain in order to enhance its security

The programs may be:

- -global, regional, national, governmental, sectoral
- multilateral, bilateral, unilateral
- compulsory, voluntary

They mostly apply to specific elements, areas, segments, sectors, links or events of the supply chain, or groups thereof. They may require the use of specific technologies or equipments, or sets thereof. (in SCS parlance, it is sometimes called “initiative”)

Recovery A return to normal from a crisis situation

Resilience Ability to recover quickly following a disruption

RF Radio Frequency

RFID Radio Frequency Identification. Technology used to track and trace shipping containers

Risk Management The human activity which integrates recognition of risk, risk assessment, developing strategies to manage it, mitigation of risk using managerial resources into a prioritization process (adapted from Wikipedia)

Risk Matrix A tool for conducting Risk Assessments and presenting the findings, showing the severity of the consequences and the probability of mishap

ROI Return on Investment

SAFE World Customs Organization (WCO) Framework of Standards to Secure and Facilitate Global Trade

Scanning Commonly called non-intrusive inspection (NII) and refers to non-destructive methods of inspecting and identifying goods in transportation systems. It is often used for scanning of intermodal freight shipping containers. In the US the main purpose of scanning is to detect for radioactive or nuclear materials with the added bonus of detecting other types of suspicious cargo. In other countries the emphasis is on manifest verification, tariff collection and the identification of contraband

Screening (1) Customs and Border Patrol (CBP) defines screening as a passive means of scanning a conveyance, baggage or cargo. CBP screens conveyances, baggage, and cargoes with

	radiation portal monitors and other radiation detection equipment for the presence of radiological emissions — i.e., nuclear screening
Screening (2)	CBP also use the term "screen" to describe the targeting and risk management process. CBP screens information on 100% of import containers through its ATS (see above) 24 hours before they are loaded onto US-bound vessels. Each and every container identified as high risk is subsequently inspected either in the foreign port of loading or upon arrival in the U.S. by CBP. (see Inspecting and ACI)
SCS	Supply chain security. The process used to secure against network disruptions throughout the supply chain
SCSM	Supply chain security management
SFI	Secure Freight Initiative – US security initiative to secure cargo coming in the USA
Single Window	A concept for trade facilitation that refers to the use of a single electronic location for providing and receiving standardized information
Smart Container	Container equipped with built-in internal sensors for security. A Smart Container may include a navigation and routing guidance system, satellite location, secure the box origin to destination and radio frequency identification
SPA	Safe Port Act of 2006 (US)
SOLAS	International Convention for the Safety of Life at Sea (SOLAS) is the most significant treaty addressing the safety of cargo vessels
SSCC	Serial Shipping Container Code
SSTL	Smart and Secure Trade Lanes Pilot Project
STAR	Secure Trade in the APEC Region – focused on securing Asia-Pacific trade while protecting regional transportation networks
TAPA	Technology Asset Protection Association. A global association of companies that contribute to exchange information between companies and authorities and which has drawn up security standards, principally for road transports of high-value goods
TEU	Twenty-foot Equivalent Unit equals the volume of one standard twenty foot container. This is used as measurement for freight volume
Threat assessment	The process of identifying potential threats, conducting a probability analysis of the realization of those threats, and forecasting the impacts of those threats
TQM	Total Quality Management
TSR	Freight Supplier Minimum Trucking Security Requirements. An initiative which was introduced when TAPA was established with criteria and minimum requirements in respect of security standards specifically directed towards truck transports of goods

UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
VAT	Value added tax
Vulnerability	The level of exposure to disruption in the supply chain
WCO	World Customs Organization
WLAN	Wireless Local Area Network
WTO	World Trade Organization
XML	Extensible Markup Language

ANNEX III Main Regional and National SCS programs

1 Frontline(1991)

Frontline, begun and regulated by Australian Customs, is a program of cooperation with companies within the country aiming to enhance security in the supply chain. According to the Australian Customs, Frontline is a program that is based on trust and the dissemination of information. Rather than focusing on strengthening security in container traffic, Frontline focuses on preventing illegal imports and exports through the collection of information from partner companies. Indicator sheets, published by Australian Customs, which all participants in the program have access to, act as guidelines for companies to assess activities in respect of air traffic, goods transportation, terminal container handling, ships on international journeys, and Customs clearance procedures. Membership is free and currently there are over 700 member companies involved. Companies that are involved in international trade and transport can become members of Frontline.

2 Business Alliance for Secure Commerce (BASC)(1996)

The Business Alliance for Secure Commerce (BASC) was created in 1996, initially as an anti-smuggling alliance . BASC's creation followed the submission of a proposal by Mattel Corp, a North American company, to the US Customs concerning the implementation of SCS procedures to reduce the risk of legitimate cargo being used by illegal organizations for narcotics trade, cargo theft and contaminated cargo". Since then, BASC has expanded its vision and dimension into a business alliance with an aim to facilitate and promote world trade by establishing and administrating global SCS standards and procedures, in partnership with business, governments, Customs, law enforcement agencies and international business organizations.

BASC's members are to be found in the private and public sectors, and among international organizations and associations. The private sector is represented by companies in the international supply chain that are active in logistics and other activities in international trade. Customs authorities and international police organizations represent the public sector. The vast majority of its participants are from Latin American companies, although participants from other regions are involved. In Europe, France, for example, is a member of BASC since its Customs authority has joined the program. The WCO and the US's Chamber of Commerce are two examples of organizations and associations that participate in BASC. Special requirements entail that participants be a company or a person actively involved in logistics, production or service activities related to foreign trade or services. Furthermore:

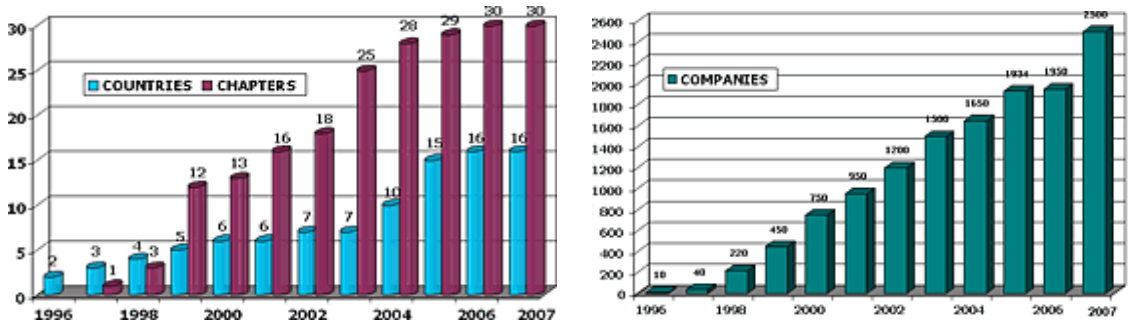
Each company must be legally established and have commercial activities in the country and overseas, that will permit the validation of the integrity of the firm, their partners and directors. Also, the company should not have any criminal record or considered to have by any national or foreign authorities a suspicious person(s) and/or dubious legal or criminal reputation.

Each company must comply with the registration process approved by each chapter according to the procedure set by the World BASC Organization.

BASC member companies are "*periodically audited and warrant that their products and services are produced and delivered under strict security controls and monitored at every step of the transportation process, using a range of security systems and processes". According to BASC "membership emphasizes a company's*

commitment to expand control of its business environment and therefore control those factors that affect the economic, fiscal and commercial interests of a country" (BASC Alliance for Secure Commerce).

Figure III-1 Evolution and Growth BASC 1996 - 2007



Source: BASC Alliance for Secure Commerce, *What is BASC?*

As the above diagram explains, BASC has witnessed significant annual rises in countries and companies involved in the program. In particular, 2003 was of particular significance for the "growth and recognition of BASC around the world, marked by trends in international trade, the challenges of globalization and at the same time, the new security regulations implemented by the US government and entities such as the International Maritime Organization and the World Customs Organization)".

Due to the demands of annual growth and BASC's commitment to its stated "objective of creating an international entity that would provide oversight the functioning and credibility of the program at the international level", the World BASC Organization (WBO) was legally constituted in 2002 in the US. The WBO is a non-profit organization which aims "to secure and facilitate international trade by the establishment and administration of global security standards and procedures applied to the supply chain in association with Customs administrations and government authorities". BASC has evolved towards securing the integrity of the supply chain and promoting mechanisms to integrate companies, governments, Customs services and international organizations.[39]

3 APEC/STAR (1997)

Asia Pacific Economic Cooperation (APEC) is an economic forum for countries situated in the Asia/Pacific region.[40] The member states discuss matters that concern the regional economy, cooperation, trade and investments. Regarding security for transport and travel, APEC has organized STAR conferences since 2003, which were created as a reaction to the terrorist attacks of 9/11 with the purpose of creating an "action plan which aims to enhance security for goods, ships, aircraft and passengers with the aid of a number of security measures". APEC's SSC guidelines encompass the following:

[39] This section is based primarily from information gathered from BASC website. For more information see http://www.wbasco.org/english/what_is_basc.html

[40] APEC's member states are Australia, Brunei, Chile, the Philippines, Hong Kong, Indonesia, Japan, Canada, China, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Russia, Singapore, South Korea, Thailand, USA and Vietnam.

- Physical security
- Access control
- Personnel
- Education, training and awareness
- Security procedures
- Document handling
- Trade partner security
- Transport security
- Crisis management and recovery after crises (Kommerskollegium, 2008).

In the action plan of STAR it is recommended that companies, in accordance with their own needs, comply with these security measures, and comply with international standards and requirements laid down by the WCO, IMO, ISO. However, no formal agreements have been made. The US is "playing an important role in this program of cooperation and has succeeded in introducing the CSI in most major ports in the region", along with being a "driving force behind APEC's action plan". (Kommerskollegium, 2008)

4 Secure Export Partnership (SEP) (2004)

The Secure Exports Scheme is a voluntary arrangement between exporters and the New Zealand Customs Service, designed to protect the exporters' international trade through the supply chain against tampering, sabotage, smuggling and other trans-national crime. The purpose of the SES is to ensure that goods to be exported are packaged securely, with no other goods and conveyed to the place of shipment securely and without interference, before shipping.

New Zealand Customs Service aims to secure supply chains from packing to loading for export, and charges for the storage of export goods will be lower, for one, by companies been given so-called "Green Lane" status, meaning that cargo can be moved to a port or airport with little chance of Customs controls (NZ Customs).[41]

NZ Customs Service signed a Mutual Recognition Arrangement (MRA) with US CBP in Brussels in 2007. This is a 'world first' SCS mutual recognition arrangement between customs administrations since the adoption of the WCO's FoS to Secure and Facilitate Global Trade. It is anticipated that this acknowledgement by both administrations of their respective customs-to-business supply chain security programs will benefit both industry and government.

5 Golden List Program (2005)

Initiated in Jordan in 2005, the Golden List program is a government-led program aiming to enhance SCS. The program is regulated by Jordan Customs and covers import and export routes for companies in Jordan. A major idea behind the program is to attract foreign investors by creating a more secure investment environment. The program is based on risk management and fulfillment with Customs requirements, and international security standards. Companies that are active in importing, exporting, Customs clearance, transport management or warehousing, and have introduced and followed certain security and trade measures, shall enjoy a large number of benefits in the form of simplified routines. To be approved for the

[41] This information is obtained from the NZ Customs website. For further information see New Zealand Customs Services's Fact Sheet 34 – Secure Export Scheme.
http://www.customs.govt.nz/library/Fact+Sheets/Fact+Sheets.htm

Golden List, a company must have sufficiently large trade volumes. The Golden List program is still in its pilot phase and only 15 companies are currently involved in the program.

6 **Secure Trade Partnership** (STP) (2007)

Commencing on 25 May 2007, the STP is a voluntary certification program administered by Singapore Customs that encourages companies to adopt robust security measures in their trading operations, thereby contributing to the improvement in the security of the global supply chain". Moreover, STP "provides companies with a framework to guide the development, implementation, monitoring and review of their supply chain security measures and practices". Through the STP program, Singapore Customs seeks to:

- Create awareness of the importance of total supply chain approach to cargo security
- Encourage companies to play their part in securing their own processes within supply chains
- Enhance the security of global supply chain and prevent disruptions to the smooth flow of goods, and profile Singapore as a secure trading hub.[42]

According to the Singapore Customs, STP is consistent with the WCO's SAFE FoS. The purpose of STP is not to override other security initiatives that companies may have introduced; Customs will take into consideration existing certificates that companies have received, on the condition that the requirements in these overlap the requirements in STP.

Currently there are 22 partners involved, and the program is open to all supply chain stakeholders, including, importers, exporters, warehouse operators, transporters, and terminal operators, etc, involved in sea transport routes to Singapore. According to Singapore Customs, "by participating in the STP program, companies will be demonstrating their commitment to adopting and implementing appropriate security measures and a willingness to assume responsibility for keeping their supply chains secure".

7 **Modernized Partners in Protection (PIP)(2008)**

The Modernized Partners-in-Protection (PIP) program, launched in June 2008, moves away from the initial goals of the PIP program of promoting business awareness and compliance with customs regulations, to a program that strengthens SCS. Regulated by the Canada Border Services Agency (CBSA), the new PIP certification program includes minimum security requirements, mandatory site validations, an appeals process and an automated application process. The goal of the restructuring of CBSA's PIP program was to foster Mutual recognition between PIP and US Customs and Border Protection (CBP) C-TPAT program.

Obtaining a PIP certification requires an organization to complete a security profile for their main operations and security profiles for all subsidiary and/or affiliates with different business numbers. The completed security profile must clearly demonstrate that all security requirements have been met. CBSA will then work with the organization to conduct site visits, review the security profiles, and offer suggestions to correct areas that received high Risk Assessments.[43]

Table III-1 Summary of the major regional/national voluntary programs

[42] This section is based primarily from information gathered from a Singapore Customs document titled Secure Trade Partnership, available at http://www.Customs.gov.sg/leftNav/trad/Supply+Chain+Security.html

[43] See Canada's Border Services Agency information on PIP for further details
: http://www.cbsa-asfc.gc.ca/security-securite/pip-pep/menu-eng.html

Name/ Abbreviation/ Start year	Originated Country/ Institute	Regulating body	Covered route	Transport mode	Participation / Status	Category	Goal
Frontline, 1991	Australia	Customs	Import and export in Australian companies	All	700 Companies	Govt. Voluntary	Prevent illegal imports and exports
BASC, 1996	Latin American trade	BASC	Latin America to North America	Mostly sea (also land and air)	1500 Companies	Private/ Voluntary	SCS and Partnership
APEC/ STAR, 1997	Australia	APEC observers	Pacific Ocean Area	Sea and air	21 member countries	Intl- Voluntary	Economic growth and partnership
SEP, 2004	New Zealand	Customs	NZ to any country (export)	All	Limited information	Govt.- Voluntary	Protect cargo against crime
Golden List, 2005	Jordan	Customs	Import and export in companies in Jordan	Pilot phase, can cover all.	15 companies	Govt.- Voluntary	Securing the supply chain
STP, 2007	Singapore	Singapore Customs	Import, export and transit in Singapore	Sea	22 partners	Govt. Voluntary	Awareness program, establish Singapore as a secure trading hub
Modernized PIP 2008; updated from 1995 PIP	Canada	Canada Border Services Agency (CBSA)	Import to Canada	All	Limited information	Govt.- Voluntary	Business awareness and compliance with Customs regulations

ANNEX IV SCS Implementation Checklist

CHECKLIST FOR GOVERNMENTS AGENCIES (a.o. Customs)

1) **Strategic Management**: Customs should have a border security policy and a Strategic Plan which provides goals, objectives and priorities regarding SCS. Customs facilities are supposed to meet international security standards imposed by (ISPS Code), International Civil Aviation Organization (ICAO), etc. For this purpose, border posts and Customs offices should be suitably located and have satisfactory conditions to carry out examination and inspection. Technical specifications, tools and equipment for the inspection and examination of goods/means of transport are required to be available in border posts and/or Customs offices. Furthermore, non-intrusive inspection (NII) equipments and a sufficient computerized infrastructure would strengthen the physical resources.

2) **Resources**: Customs has to have both physical and human resources to carry out its SCS responsibilities. A Customs administration is expected to have sufficient expertise to identify and manage SCS risks. Basic training for operational and specialist staff should include sessions on SCS.

1. Legal Framework

National legislation should give Customs the administrative power for examination, detention and seizure of goods and means of transport, as well as inspection of cargo and entire Customs territory. There should be some national legislation allowing Customs officials to obtain information on goods and means of transport prior to their arrival in the territory. The legal framework should enable the information/intelligence exchange with other Customs and non-Customs organizations and the protection of confidentiality of Customs data.

2. Intelligence and Risk Management

The Customs administration is expected to develop a national strategic risk management policy that takes into account SCS initiatives and use this policy to ensure the selectivity of Customs controls focusing on high risk areas. The national administration should encourage using IT systems for risk management purposes. The risk management system and its components should regularly be maintained and updated.

3. Information and Communication Technology

The administration should apply the internationally accepted data standards, such as the WCO Data Model, the Unique Consignment Reference Number (UCR), etc. and have an Information and Communication Technology (ICT) security policy.

4. External Cooperation, Communication and Partnership

The administration is supposed to use multilateral or bilateral Mutual Administrative Assistance (MAA) agreements to exchange information or intelligence on supply chain security. Common approach for risk management and controls with other Customs administrations should be adopted. Customs should have partnership programs as structured in AEO, C-TPAT and similar partnership schemes.

5. Integrity

The high level management staff of the Customs administration should support anti-corruption activities and demonstrate integrity and leadership in combating corruption. Customs has to have action plans for anti-

corruption purposes. The overall Customs practices must be reviewed to check legislation discretionary power to Customs officers, increasing excessive bureaucracy and unnecessary duplications.

As complementary to above mentioned requirements, the Customs administration should maintain performance measures especially on examination processes and should work with other competent authorities to conduct security assessments involving the movement of goods in the international supply chain and commit to resolving identified gaps expeditiously.

In conclusion, Customs authorities should follow the basic principles for their actions to maximize international SCS by considering the following requirements:

- Strategic planning
- Conducting supply chain Risk Assessments
- Reflecting the Risk Assessment results into national, regional and global plans Programs and legislation
- Evaluate the Risk Management results on the high risk area and prioritize the outcomes
- Implementation of SCS practices
- Encourage businesses to adopt a SCS standard, initiative or program
- Assist business sectors to follow the adopted practices in their operations
- Improve and help to improve physical security infrastructure of international trade ports
- Provide guidance to businesses to adopt secure IT and data systems to promote SCS
- Provide training/education to both government and private sector personnel related to SCS
- Ensure the quality level of SCS practices through audits and investigations
- Continuous review of the overall SCS system and improvement of the system according to emerging needs.

SCS IMPLEMENTATION CHECKLIST FOR BUSINESS OPERATORS *44*

This checklist was constructed by the APEC private sector and is a combined approach from the following references: Business Anti-Smuggling Coalition (BASC) Security Program, Customs-Trade Partnership Against Terrorism (C-TPAT) guidelines, 2003 World Customs Organization (WCO) Supply Chain Security and Facilitation Advance Cargo Information guidelines, IBM Corporate Security guidelines. Elements of SCS pertain differently to each organization. Each organization should focus on elements of the highest importance. Complex, multi-country supply chains demand more collaboration on security issues. Security inside the organization is not sufficient. Collaboration outside the organization is essential. Businesses should conduct security assessments and implement security plans with regular updates. Most importantly, businesses need to comply with international standards and requirements set by the WCO, the IMO, the ISO, etc. The following 9 elements are highlighted below in order to provide a generic checklist, including the key elements of supply chain security.

1. Physical Security

Physical security includes security measures that monitor and control the facility's exterior and interior perimeters. This will include mail service security, lock and key control, and perimeter and interior alarms. Recommended features, to be installed as appropriate:

[44] http://www.asianlii.org/apec/other/agrmt/apsscsg519/

- Appropriate peripheral and perimeter barriers
- Electronic security systems, to include theft alarm systems, access control systems, closed circuit television (CCTV)
- Clear identification of restricted areas
- Locking devices on external and internal doors, windows, gates and fences. Exterior doors and windows should be equipped with alarms
- Segregated and marked domestic, international, high value, and dangerous goods cargo areas within the warehouse, preferably by a safe, caged or otherwise fenced-in area
- Emergency lighting / power systems for key operational areas and high value cargo areas
- Periodic inspection and repair to assure integrity of security measures.

Recommended procedures, to be conducted as appropriate:

- Depending upon its size, the company may require a security organization
- Gates or doors through which vehicles or personnel enter or exit should be manned or under observation by management or security personnel
- Access to employee parking should be controlled
- Employee parking should be separated from visitor parking
- Private passenger vehicles should be prohibited from parking in cargo areas or immediately adjacent to cargo storage buildings
- Lock and key control, including signing in and out of high-risk areas
- Restrict access to document or cargo storage areas.

2. Access Control

Access controls prohibit unauthorized access to facilities, conveyances, vessels, aircraft, shipping, loading docks, and cargo areas. If access control is not possible, increased precautions in other security aspects may be needed. Recommended procedures, to be conducted as appropriate:

- Use of access control points and the positive identification, recording, and tracking of all employees, contractors, visitors and vendors
- Access control system for persons and vehicles
- Procedure to challenge unauthorized / unidentified persons
- Deny access and trigger an alarm when visitors attempt to enter an unauthorized area
- Inspect vehicles required to access operations areas
- Control the times individuals have access to facilities
- Post a map of restricted areas within view of employees and visitors.

3. Personnel Security

Personnel security is concerned with the screening of employees and prospective employees, as appropriate and as allowed for by law. Recommended procedures, to be conducted as appropriate:

- Review skill requirements for key positions
- Verify job application information
- Check background of employees in sensitive positions
- Contact references
- Investigate criminal records, if any

- Assure correct alignment of job skill requirements with individual's skills
- Conduct periodic background checks, note unusual changes in social and economic situation
- Check background and corporate structure of independent contractors
- Implement drug consciousness programs
- Drug testing, as allowed for by law
- Before hiring
- Random periodic testing
- At times of reasonable suspicion
- Employee identification (ID) procedures
- ID cards or bracelets
- Different color ID cards to designate access privileges
- Different color uniforms for each sensitive area
- Different color uniforms for security staff
- Gate passes should be issued to truckers and other onward carriers to control and identify those authorized to enter the facility.

4. Education, Training and Awareness

Education, training and awareness encompass education and training of personnel regarding security policies, encouraging alertness for deviations from those policies and knowing what actions to take in response to security lapses. Recommended procedures, to be conducted as appropriate:

- Communicate security policies and standards to employees, including consequences of noncompliance
- Participation of all personnel in security awareness and training programs
- Recognition for active employee participation in security controls
- Incentives for individuals or employees reporting suspicious activities
- Use press releases, email distribution lists and bulletin boards.

5. Procedural Security

Procedural security assures recorded and verifiable location of goods in the supply chain. Procedures should provide for the security of goods throughout the supply chain and contingency procedures should be included within the scope of procedural security. Recommended procedures, to be conducted as appropriate:

- Record and verify introduction of goods into the supply chain under the supervision of a designated security officer
- Record and verify removal of goods from the supply chain under the supervision of a designated security officer
- Protect against not manifested material being introduced into the supply chain
- Properly store empty and full containers to prevent unauthorized access, including the use of tamper-proof / non-counterfeitable seals
- Check empty containers received for storage or loading to assure its structure has not been modified
- Establish procedures for affixing, recording, tracking, and verifying tamper-proof / non-counterfeitable seals on containers, trailers and railcars. Seals should not be used in strict numeric sequence nor should seals be registered and controlled by a single person

- Verify the identity and authority of the carrier requesting delivery of cargo prior to cargo release
- Procedures for detecting shortages, overages, irregularity or illegal activities
- Procedures for notifying Customs and other law enforcement agencies of suspected illegal activities
- Proper marking, weighing, counting and documenting of cargo / cargo equipment, verified against manifest documents
- Procedures for tracking the timely movement of incoming and outgoing goods
- Random, unannounced security assessments
- Inspection of persons and packages
- Additional security procedures for high-value and high-risk goods.

6. Documentation Processing Security

Documentation processing security, both electronic and manual, assures that information is legible and protected against the loss of data or introduction of erroneous information. Recommended procedures, to be conducted as appropriate:

- Safeguard computer access and information
- Control access to information systems, both by level of job responsibility and level of information sensitivity
- Physical security in computer areas
- Monitor employee use of data systems
- Processes to backup computer system data
- Record the amount of cargo by packing unit type, packing conditions, and security seal stamps. Discrepancies should be recorded with a note, photograph and scale weight records
- Signatures required for all process checkpoints like document preparation, when seals are applied/broken, truck inspection, opening the vault, cargo delivery, cargo receipt, counting unshipped pieces
- Fix times for the preparation of documents and for the shipping and unloading of cargo
- Use special control procedures to prepare emergency/last-minute shipments and if necessary notify authorities regarding such shipments
- Software systems should register transactions or support operations and, if possible, make a follow up of the activities that it handles
- Record the entrance and exit time of people receiving and delivering goods
- Document significant process delays
- Ensure that manifests are complete, legible, accurate, and submitted in a timely manner
- Future automated data exchange related procedures
- Establish electronic Customs reporting systems based on WCO Customs Data Model and the Unique Consignment Reference
- Establish advance manifest reporting systems.

7. Trading Partner Security

- Trading partner security extends SCS to suppliers and customers. Communication, assessment, training, and improvement are key components. Recommended procedures, to be conducted as appropriate: 1) Encourage trading partners/suppliers/contractors to assess

and enhance, if required, their supply chain security; 2) Request written security agreements with trading partners/suppliers/contractors to include controls such as:

- Tamper-proof/non-counterfeitable seals
- Signatures
- Time controls
- Agreed means of communication
- Consider offering incentives to trading partners/suppliers/contractors for enhanced security coordination and cooperation
- Document mutual SCS policies
- Extensive exchange of information between trading partners/suppliers/contractors
- Advise Customs and foreign authorities of security agreements with trading partners
- Education, training and awareness by trading partners on SCS
- If possible, include equivalent security provisions as a condition of contract for contractors / suppliers providing services.

8. Conveyance Security

Conveyance security provides protection against the introduction of unauthorized personnel and material into the supply chain, including the areas between the links of the supply chain. Recommended procedures, to be conducted as appropriate:

- Routinely search all readily accessible parking, storage, loading and transit areas
- Secure internal/external compartments and panels
- Procedures for reporting instances in which unauthorized personnel, not manifested materials, or signs of tampering of a conveyance are discovered
- When high-value or high-risk cargo must be transported a substantial distance from the point of unloading to a special security area, vehicles capable of being locked or otherwise secured should be used
- Use locks, tamper-proof/non-counterfeitable seals or electronic seals to secure conveyances
- If cost-effective, use transponders to facilitate continual tracking of conveyances
- Use automatic electronic transmittal of 'smart card' data to Customs if available
- Use 'smart card' technology containing vehicle, consignment, and driver information where automated border crossings are in place
- Consider cost and future standardization issues related to use of smart cards, electronic seals and transponders
- Stay informed regarding development of standards and requirements regarding smart cards, electronic seals and transponders by WCO, IMO, ISO, etc.

9. Crisis Management and Disaster Recovery

Crisis management and disaster recovery procedures include advance planning and process establishment to operate in extraordinary circumstances. Recommended procedures, to be conducted as appropriate:

- Emergency Plan
- Crisis Management Team (CMT)
- Emergency response personnel in-house
- Periodic updates and walk-through
- Crisis management rooms

- Primary and alternate off-site locations
- Training Periods
- Emergency response personnel
- Testing
- Compliance reporting
- Senior location leadership certification - all locations
- Incident tracking and information coordination
- Investigation capability and follow-up
- Law enforcement role and linkage
- Analysis of cause of crisis.

Transport Division

Energy, Transport and

Water Department

The World Bank

1818 H Street NW

Washington DC 20433

USA

www.worldbank.org/TRS