SEVENTH FRAMEWORK PROGRAMME
SST–2007–TREN–1 SST.2007.2.2.4 Maritime and logistics co-ordination platform
SKEMA Coordination Action
"Sustainable Knowledge Platform for the European Maritime and Logistics Industry"

SKEMA Policy Study

Supply Chain Security: The US, EU and International Regulations

This SKEMA policy study aims to introduce the supply chain security regulations for the sea transportation. It draws original information from a number of SKEMA studies and other international official sources. It explores new developments that took place in 2011 and early 2012. It provides an extensive overview of the existing regulatory frameworks and the attempt for harmonisation of regional and international regulations by various authorities.

Document Summary Information

Version	Authors	Description	Date
1.0	V. Bojkova, Inlecom	Final	13/02/2012

Supply Chain Security:
The US, EU and International Regulations

Global companies and suppliers need a secure chain to protect their assets and profitability. Any business that imports or exports products, finished goods or components, by sea or air, has to follow certain requirements. These rules vary in accordance with the transport mode. In air transportation, the focus is extensively on air cargo security while in the sea transportation, the focus is primarily on port and container traffic security.

In this respect, the intention of this Policy Paper is to present the US, EU and international regulations that define and monitor supply chain security in the sea transportation area. Programmes, initiatives, recent actions and regulations are to be thoroughly explained and discussed through the paper. As it will be noticed there is a great deal of rules under differing authorities.

Ports security interacts with a few programmes such as the US Customs – Trade Partnership Against Terrorism (C-TPAT); the World Customs Organisation (WCO) standards for supply chain security; the Container Security Initiative (CSI); the EU Authorised Economic Operator Initiative; the International Ship and Port Security code and EC Legislation 725/2004.

In the field of container security, the Global Shipment Identification Number (GSIN) enables the identification of grouped transport units that travel under one commercial order. It helps the Customs Organisations to process thousands of national and international transactions daily. Additionally, the International Organisation for Standardisation has a group of standards for container traffic and risk management, for example:

1) ISO 31000 series – risk management;
2) ISO 28000 series – supply chain compliance support;
3) ISO 18185 series – shipping container e-seals standard[1];
4) ISO 18186 – RFID cargo shipment tag system[2];
5) ISO 17712 – Freight containers, Mechanical seals[3];
6) ISO/IEC 15961/2 series – RFID item management;
7) ISO 6346 – Shipping container marking/coding standard;
8) ISO 1496 series – Freight containers, Specification and testing;
9) ISO 668 – Shipping container dimensions standard.

All these measures undertaken by national governments, international authorities and customs to guarantee secured transportation regulate the global supply chain heavily. The US and EU authorities share a common approach to the security of the supply-chain and demand implementation of mutual recognition of the relevant US C-TPAT and EU AEO programmes[4].

---

[1] For more details, see SKEMA study "Practical examples and experiences of visibility systems deployments", Study produced by VTT, Finland

[2] SKEMA op. cit.

[3] SKEMA op. cit.

[4] See details at: www.dhs.gov and www.ec.europa.eu

The EU-member states that do not meet security requirements have been asked to apply measures fully in order to improve the supply-chain security level. For instance, in 2011 the Commission asked Sweden to improve port security by implementing Directive 2005/65/EC, which was based on Regulation 725/2004 for enhancing ship and port facility security[5].

I. The US Security Regulatory Framework

In more details, the US C-TPAT programme is the largest government-private sector partnership that was launched at the end of 2001. It is based on voluntary principles and includes more than 7,500 companies from the supply chain that jointly developed security criteria, best practices and implementation procedures. C-TPAT speeds the shipments across and through all ports of entry, the US seaports and airports. The current security guidelines for C-TPAT members address a broad range of topics such as personnel, physical and procedural security; access controls; education, training and awareness; manifest procedures; conveyance security; threat awareness; and documentation processing. Companies that apply to C-TPAT always sign an agreement that commits their organisation to the programme's security guidelines. These guidelines offer a customised solution while providing a clear minimum standard that approved companies must meet[6].

The US Customs Service had created the Container Security Initiative too. Its three core components are:

- Identify high risk containers via automated targeting tools;
- Prescreen and evaluate containers at the port of departure;
- Use technology to prescreen high-risk containers;

Table 1: Operational Ports in Europe under the CSI

Country	*Port*
Belgium	Antwerp and Zeebrugge
France	Le Havre and Marseille
Germany	Bremerhaven & Hamburg
Greece	Piraeus
Italy	La Spezia, Genoa, Naples, Gioia Tauro, Livorno
Netherlands	Rotterdam
Portugal	Lisbon
Spain	Algeciras, Barcelona, Valencia
Sweden	Gothenburg
UK	Felixstowe, Liverpool, Thamesport, Tilbury, Southampton

Source: www.cbp.gov

The Initiative was introduced in 2002 and many customs administrations committed to joining the CSI and operate at different stages of implementation. The CSI is now

[5] MEMO/11/408 from 16/06/2011

[6] www.cbp.gov: Securing America's borders

operational at ports in North America, Europe, Asia, Africa, the Middle East, Latin and Central America. The 58 operational CSI ports prescreen over 80% of all maritime containerised cargo imported into the US (see Table 1).

Furthermore, in January 2012, the White House released the US National Strategy for Global Supply Chain Security, which aims to foster a global supply chain system that is resilient to any threats and can recover rapidly from disruptions. The US administration promotes the cooperation with other international organisations and national governments[7].

II. The EU and International Regulatory Frameworks

To respond to supply chain security challenges, the European Commission undertook a package of measures in 2003[8]. The security amendment to the Community Customs Code was introduced in 2005 with three major changes:

- Requirement for providing information to the customs authority about the goods prior to the import to and export from the EU;
- Providing traders with trade facilitation measures (Authorised Economic Operator programme);
- Introduction of uniform Community risk-selection criteria for controls[9].

The above mentioned security amendment to the Code was fully implemented in 2006 and set out the operational details of the customs processes:

- A Common Risk Management Framework (CRMF) for the customs authorities to improve the risk-based control;
- Provisions for the Authorised Economic Operator programme;
- Providing customs with advanced information on goods brought into, or out of the European Union.

Since January 2011, the advanced information declaration has been an obligation for companies trading goods, which means that all safety and security data has to be sent in advance, if not, the goods have to be immediately declared at the border of arrival. This usually avoids any delays of the customs clearance of consignments.

The EU Customs Security Programme (CSP) covers the implementation of all security measures, particularly the commonly agreed control standards and risk indicators, as well as the trade facilitation programme.

The Authorised Economic Operator status can be granted to any economic operator established in the EU as this certificate brings simplification of the customs rules and facilitates the customs control related to safety and security. There are different categories of AEO, so the type of certificates varies in accordance with the AEO category[10].

---

[7] See more details at: www.whitehouse.gov

[8] See COM (2003) 452

[9] See Regulation 648/2005

[10] See more details in the guidelines on AEO

The customs efforts by the World Customs Organisation and the European Union try to harmonise customs rules. The WCO has developed the SAFE Framework of Standards to harmonise different sets of requirements of national customs administrations as a step to automate risk management activities.

However, still the exchange of security information between the EU and other systems is not without obstacles. For instance, in the maritime sector the SafeSeaNet applications have been implemented[11], but the information is kept separately from the customs security risk management data. There is no smooth exchange of container security data between EU platforms and security operational systems used by ports, carriers and other stakeholders.

III. EC Regulations and ISPS Code

The International Ship and Port Security Code (ISPS Code) is an extensive set of measures to enhance the security of ship and port facilities. It has two parts, one mandatory and one recommendatory. Its aim is to provide a standardised framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ship and port facilities through determination of appropriate security levels.

To enhance ship and port facility security in the face of threats, Regulation 725/2004 provided the basis for implementation and Community monitoring of the special measures to enhance maritime security adopted by the Diplomatic Conference of the IMO (2002), which established the ISPS Code.

Each Member State is required to submit necessary information to the IMO in respect of taken special measures to enhance maritime security of the SOLAS Convention of the IMO. These measures are specified in Annex 1 of this Regulation 725/2004. Also each Member State has to submit a list of port facilities concerned on the basis of port facility security assessments carried out, and to establish the scope of the measures taken to apply the provisions of this Regulation. Any ship, subject to the special measures of the SOLAS Convention and the ISPS Code that intends to enter a port of a Member State, has to provide the necessary information of the special measures to enhance maritime security to the competent authority of that Member State. Member States may exempt scheduled services between ports facilities located on their territory from requirements if certain conditions are met (See Article 7).

In order to monitor the implementation of this Regulation, each Member State has to adopt a national programme. The Commission, in cooperation with the focal point is authorised to make inspections on port facilities and relevant companies, in order to monitor the application of the Regulation. The Commission is required to communicate the inspection report to the Member State concerned, which will have to provide sufficient details of any measures taken to remedy any shortcomings within three months of issued report's receipt. Moreover, the Commission may adopt provisions in order to define harmonised procedures for the application of the mandatory provisions of the ISPS Code, without broadening the scope of this Regulation. The Commission is also required to cooperate with other international organisations in order to define a

[11] See SKEMA study "Practicalities of using SSN and safety/security support systems in Latvia", Study produced by Maritime Administration in Latvia

common position or approach in the competent international area of the maritime security.

In 2005, Directive 2005/65/EC on enhancing port security came into force and a revised Regulation (EC) No 324/2008 was adopted on 9 April 2008 to incorporate procedures for monitoring Member States' implementation of the Directive jointly with the Commission's inspections under Regulation 725/2004. Now inspections are coordinated and prepared by the Commission on the basis of this legislation. The European Maritime Safety Agency provides technical assistance to the Commission, particularly involvements with the inspection tasks of ships, relevant companies and Recognised Security Organisations (RSOs) authorised to undertake certain security-related activities.

Further security requirements have been implemented in the EU based on Directive 2005/65/EC on enhancing port security. These rules require that Member States extend security measures from the ship-port interface (the port facility) to the whole port area and they will further enhance maritime security across the EU.

IV. ISO's Series of Standards on Supply Chain Security

ISO's Standards are sets of comprehensive rules and requirements specifying concrete operational actions that have to be taken in order to implement a particular policy or comply with regulatory, legal or other measures to which the organisation subscribes. There are a number of standards that address the issues of supply chain security in very detailed ways (See Table 2 and 3 below).

The two main series ISO 28000 and ISO 31000 are discussed and presented in Table 2. They relate to the security and risk management of an organisation. The ISO 28000 series specify the requirements for a security management system including the aspects that are critical to security assurance of the supply chain. These other aspects should be considered directly, where and when they have an impact on security management including the transportation of the goods along the supply chain. This standard is applicable to all sizes of organisations and any organisation needs to have its certified security management system by an Accredited Third Party Body or make a self-declaration of conformance.

The ISO 31000 series provide the principles and generic guidelines on risk management. It can be applied to any type of risk as it is intended to harmonise risk management processes. It provides a common approach in support of standards dealing with specific risks and sectors, and does not replace those standards.

Table 2: ISO's Standards on Supply Chain Security Management

ISO Standard	*Regulated Area*
ISO 28000: 2007	Specification for security management systems for the supply chain
ISO 28001:2007	Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance
ISO 28002:2011	Security management system for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use
ISO 28003: 2007	Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems
ISO 28004:2007	Guidelines for the implementation of ISO 28000
ISO 28005-1:2014	Under development This Standard is officially expected to be published in 2014. Security management systems for the supply chain – Electronic Port clearance – Part 1: Message structures
ISO 28005-2:2011	Security management systems for the supply chain – Electronic Port clearance (EPC) – Part 2: Core data elements;
ISO 31000:2009	Risk management – Principles and guidelines
ISO Guide 73:2009	Risk management – Vocabulary
ISO/IEC 31010:2009	Risk assessment techniques

Source: www.iso.org

Another group of standards is presented in Table 3 and they strictly relate to the container security such as e-seals, supply chain application of RFID[12]; processing data and its presentation to the RF tag, processing data captured from the RF tag and others. The two main series ISO 18185 and ISO 15961/2 are discussed and presented below.

[12] See SKEMA study "Drivers for the deployment of RFID (technological and cost advancements)", Study produced by VTT, Finland

Table 3: ISO's Standards on Container Security

ISO Standard	*Regulated Area*
ISO 18185-1:2007	Freight containers – Electronic seals – Part 1: Communication protocol
ISO 18185-2:2007	Freight containers – Electronic seals – Part 2: Application requirements
ISO 18185-3:2006	Freight containers – Electronic seals – Part 3: Environmental characteristics
ISO 18185-4:2007	Freight containers – Electronic seals – Part 4: Data protection
ISO 18185-5:2007	Freight containers – Electronic seals – Part 5: Physical layer
ISO/TS 10891:2009	Freight containers – RFID – Licence plate tag
ISO 18186:2011	Freight containers – RFID cargo shipment tag system
ISO 17712:2010	Freight containers – Mechanical seals
ISO 17363:2007	Supply chain applications of RFID – freight containers
ISO/IEC 15961:2004	(IT) RFID for item management – Data protocol: application interface
ISO/IEC 15961-1	Under development (IT) RFID for item management – Data protocol – Part 1: Application interface
ISO/IEC 15961-2:2010	(IT) RFID for item management – Data protocol – Part 2: Registration of RFID data constructs
ISO/IEC 15961-3:2010	(IT) RFID for item management – Data protocol – Part 3: RFID data constructs
ISO/IEC 15961-4:2010	Under development (IT) RFID item management – Data protocol – Part 4: Application interface commands for battery assist and sensor functionality
ISO/IEC 15962:2004	(IT) RFID item management – Data protocol: data encoding rules and logical memory functions
ISO/IEC 15459-2:2006	(IT) Unique identifiers – Registration procedures

Source: www.iso.org

The ISO 18185 series provide a system for the identification and presentation of information about freight container electronic seals. The information is delivered through a radio-communications interface providing seal identification and a method for determining whether a freight container's seal has been opened. This Standard consists of five parts and they are used in conjunction with each other. They apply to all electronic seals on freight containers covered by ISO 668, ISO 1496 series and ISO 8323 (see Table 4). The ISO/IEC 15961 and 15962 series specify the exchange of information via a RFID system. Both are required for the complete understanding of the data protocol, but each focuses on a particular issue – ISO/IEC 15961 addresses the information interface with the application system while ISO/IEC 15962 deals with the processing of data.

Table 4: ISO's Standards on Freight Containers

ISO Standard	*Regulated Area*
ISO 8323:1985	Freight containers – Air/surface (intermodal) general purpose containers
ISO 6346:1995	Freight containers – Coding, identification and marking
ISO 1496-1:1990	Series 1 freight containers – Specifications and testing – Part 1: General cargo containers for general purposes
ISO 1496-1:1990/ Amd 1:1993	Amends sub-clauses
ISO 1496-1:1990/ Amd 2:1998	Amends sub-clauses
ISO 1496-1:1990/ Amd 3:2005	Amends sub-clauses
ISO 1496-1:1990/ Amd 4:2006	Amends sub-clauses
ISO 1496-1:1990/ Amd 5:2006	Amends sub-clauses
ISO 1496-2:2008	Series 1 freight containers – Specifications and testing – Part 2: Thermal containers
ISO 1496-3:1995	Series 1 freight containers – Specifications and testing – Part 3: Tank containers for liquids, gases and pressurized dry bulk
ISO 1496-4:1991	Series 1 freight containers – Specifications and testing – Part 4: Non-pressurized containers for dry bulk
ISO 1496-5:1991	Series 1 freight containers – Specification and testing – Part 5: Platform and platform-based containers
ISO 830:1999	Freight containers – Vocabulary
ISO 668:1995	Series 1 freight containers – classification, dimensions and ratings
ISO 668:1995/Amd 1:2005	Amendment 1
ISO 668:1995/Amd 2:2005	Amendment 2 – 45 containers

Source: www.iso.org

The standards presented in Table 4 relate to the freight containers[13] specification and classification and they are linked to the container security standards. All together these 40 standards plus amendments create the principal foundation for standardisation of dealing with security threats in the sea transportation part of the global supply chain.

[13] See more details in the SKEMA study: "Definition of Standard Ro-Ro Unit", Study produced by VTT, Finland

V. Conclusions

The US and EU authorities acknowledge that they face similar challenges and must be ready to react to terrorist attacks or abuse of the supply chain. This was expressed in a joint statement from June 2011.

The Transatlantic Economic Council[14] identified potential areas for possible actions, which were announced as part of the joint statement on supply chain security. These areas are as follows:

(1) The preparatory work on mutual recognition of the relevant US C-TPAT and the EU AEO has completed. The reciprocal benefits of qualified AEOs and C-TPAT members will be expected to begin from July 2012.

(2) Continuation of joint efforts to revise the WCO's SAFE Framework of Standards. The USA and EU must coordinate their views on the timelines and conditions.

(3) Mutual recognition of seaports, airports and customs measures and controls; examination of the future of the CSI in the European Union.

(4) Support IMO efforts to help in the implementation of the ISPS Code.

(5) Exploration of any opportunities for sharing information and conducting joint seaport and airport assessments.

(6) Several EU Member States decided to join the World Customs Organisation' s *Programme Global Shield*[15] in 2011. It aims to undertake work on explosives, which brings together experts from law enforcement, policy and regulatory authorities and serves as a channel for technical exchange in the field of security of explosives. This also includes exchanges on the proposed EU Regulation to further control shipments of explosives precursors and comparable regulations proposed by the US.

(7) Ongoing work on testing currently available radiological/nuclear detection technologies through the Illicit Trafficking Radiation Assessment Program (ITRAP+10) to identify those technologies that meet internationally recognised standards defined by the American National Standards Institute (ANSI) and the International Electro-technical Commission (IEC). Extend and intensify the US-EU bilateral dialogue and cooperation on technology (R&D joint work; share best practices, common certification practices).

The supply chain is the most globalised sector of modern economies and as such is vulnerable to attacks at different geographical points. Thus, international cooperation is absolutely needed in order to assure that nations have the resources, capabilities and authorities to combat the exploitation of the various supply chain's segments. Also the need for coordination of all differing actions, programmes and initiatives is urgent. The cooperation between the US and EU authorities is highly regarded as it stimulates

[14] The Transatlantic Economic Council is a body set up by the US and EU to direct economic cooperation and harmonise regulations between the two economies.

[15] The program began as Project Global Shield in March 2011 and then endorced by the WCO as a long-term programme. It enables customs and police to work together on stopping the illicit trafficking and diverting of precursor chemicals.

further international actions; builds the principles for protecting the global supply chain; harmonises regulations; funds many novel ideas and coordinates joint work of national and international authorities.

REFERENCES:

[1]. www.cbp.gov

[2]. www.dhs.gov

[3]. www.eskema.eu

[4]. www.ec.europa.eu

[5]. www.ec.europa.eu/trade

[6]. www.ec.europa.eu/transport

[7]. www.europa.eu/rapid

[8]. www.iso.org

[9]. www.wcoomd.org

[10]. www.whitehouse.gov