

# CARGO SECURITY

INTERNATIONAL

[www.cargosecurityinternational.com](http://www.cargosecurityinternational.com)

Volume 5 Number 1

February / March 2007

## Inside:

- Cargo Theft Gangs
- Biometrics
- Border Security
- WMD Sanctions
- Cargo Inspection
- Aviation Final Rules

**PORT SECURITY:  
Felixstowe's RHIDES**

# Is it SAFE?

*Jim Giermanski considers the genesis, current status and future of container security*

**W**hen did my cargo leave? Where is it? When will it get here? What's its condition? If it left the port two days ago, why isn't it here now? These are familiar questions to any firm depending on a global supply chain. Governments have similar questions. Who is the shipper? Where is it coming from? What do we know about this container? With the incredible increase of container volumes, seaport growth, and unpredictable seaport selection and usage, industry leaders and governments are looking for more knowledge – and they want it to be delivered as fast as possible. Customs authorities and industry leaders recognise that only an automated electronic system can monitor these volumes and the security aspects surrounding them. 9/11 increased the concern over unmonitored container movements as potential implements of terrorism.

The **World Customs Organization (WCO)** has taken the leadership role in container security, and it appears that Europe is taking the leadership role in testing satellite systems to monitor and secure global containerised shipments. Specifically, the WCO has led the movement to automate and ensure the security of cargo in a global pipeline. Its push for automated systems and electronic transfers of data, critical in accommodating the growth of the container and port industry world-wide, had its roots in the 1973 Kyoto Convention.

## Kyoto Convention

The genesis for improving and modernising Customs practices around the world was the Revised Kyoto Convention of 1999. It specifically supported the concept of applying new technology to Customs practices. The revised Kyoto Convention had the goals of simplifying Customs procedures, emphasising information technology and risk management, and using automated systems to target and select high risk shipments for inspection based on pre-arrival information. Specifically, the Kyoto Convention ICT (Information and Communication Technology) Guidelines include the advance electronic transmission of information to Customs services' computerised systems, including the use

of electronic exchange of information at export and import.

The WCO adopted the Revised Kyoto Convention on 26 June 1999 and used it as the baseline for the development of its Framework Standards to Secure and Facilitate Global Trade. The Standards were adopted by the WCO in 2005 (see *Cargo Security International*, June/July 2005, page 4). All 169 country members of the WCO unanimously adopted the Standards. There are four core elements of the Standards:

- advanced electronic manifest information requirements
- common risk management approach
- inspection of certain container by non-intrusive means
- benefits to businesses for co-operation.

The WCO has proposed programmes to 'push the security of cargo and container further back into the supply chain by involving the private sector and by requiring increased security at the point of origin, e.g. the point of stuffing a container at a foreign manufacturer's loading docks, and as the container is moved point to point through the supply chain'. The Appendix to Annex I of the Standards is dedicated to the security of containers.

## SAFE Port Act

In many ways some elements of the Standards are incorporated into recent US legislation. The SAFE Port Act was signed into law on 13 October 2006. Overall, the Act is consistent with the WCO Standards: for example, it calls for radiation detection, among many other requirements (see *Cargo Security International*, October/November, page 24). The Act provides for in-container detection as well as portal x-ray machine detection at the participating foreign ports; automated targeting; container security standards; and the codification of the Container Security Initiative (CSI) and the Customs–Trade Partnership Against Terrorism (C-TPAT). It also establishes 'green lane' provisions in the form of Tiers 1, 2, and 3. Tier-3 treatment, the greatest commercial incentive to importers and shippers, requires the use of a container security system. The Act also requires the

Jim Giermanski is the Director of the Center for Global Commerce at Belmont Abbey College.

Contact:

Jim Giermanski

Email: powersintnlinc@bellsouth.net

establishment of an electronic trade data interchange system to be known as the International Trade Data System (ITDS), and must be implemented as soon as the **Customs and Border Protection Agency's (CBP) Automated Commercial Environment (ACE) system** is fully implemented.

## Container Security Initiative

The CSI programme, an initiative set in motion by the US Commissioner of Customs after 11 September 2001, was codified into US Law in the SAFE Port Act, and supports cooperative Group of Eight (G8) action on transport security. Among its core elements are the identification of high-risk containers (advance information and intelligence), prescreening and evaluation before sailing to the United States, x-ray and gamma ray screening and the use of smarter, more secure containers. CSI is also consistent with WCO Standards, and requires that all manifest information be electronically provided 24 hours before containers are laden into a vessel at foreign ports destined for US ports. Around 50 foreign ports currently participate in the CSI programme.

## C-TPAT

What is most significant about C-TPAT is its consistency with the definition of the 'international supply chain' contained in Section 2 of the SAFE Port Act, which requires security to begin at origin, and end at destination. Rail must provide tracking information. All C-TPAT participants must move toward electronic transmission of information consistent with the new E-Manifest, a component of the ACE system.

## ITDS

The National Performance Review recommended the creation of the ITDS in 1995. Codified in the SAFE Port Act, the ITDS establishes a single portal system operated by the CBP for the collection and distribution of standard electronic import and export data required by all participating federal agencies. It will become the repository of electronic trade information generated by the Automated

Commercial Environment (ACE) system and the E-Manifest.

## ACE

The Trade Act of 2002, one of the many statutes enacted in response to 9/11, as amended by the Maritime Transportation Security Act of 2002 (MTSA), required that the CBP promulgate regulations to begin collecting all manifests electronically. All shipments without exception must include complete bill of lading information electronically entered into the ACE system.

## E-Manifest

The E-Manifest is the key electronic format that facilitates the use of the ACE system at land ports-of-entry. Examples of required entries include: driver's identification, product codes, shipper and consignee, all bill of lading data, package type, value, country codes, to name a few.

## Security/logistics nexus

While the genesis for logistics and Customs' efficiency may be Kyoto, the security genesis is certainly 9/11. From Kyoto to the E-manifest, there is a global consistency in the collection, storage, and electronic transmission of trade and manifest data from the stuffing of the container at origin to the opening of the container at destination. Data may include all types of information depending on unique government and industry requirements.

From Bill of Lading and/or Booking confirmation/Dray Order one can obtain information such as:

- identity of person supervising stuffing and arming the system at origin
- document number
- booking number
- shipper/exporter
- forwarding agent and licence number
- city or point of origin (stuffing)
- date of departure from origin (if known)
- consignee
- notify party
- place of receipt by land carrier
- exporting carrier (vessel line)
- sea port of loading (origin sea port)
- loading pier or terminal if known
- sea port of discharge

- declared value
- container identification number
- gross weights
- description of goods (six digit tariff number).

## Smart container

A smart container must perform at least seven security operations:

- it must record the identity of the person supervising the loading and arming the container at the foreign port of origin
- it must provide for electronic capturing of certain trade data that will link to other documentation
- it should be able to detect a breach anywhere into its body, not just through the doors
- it should be able to report a breach in real time or close to real time with the date, time, and geographic location of the breach
- it should be able to give its geographic position throughout the supply chain when queried, or automatically give its position when it is off its designated course of travel
- it should recognise and record the identity of the authorised person opening the container at destination
- finally, it should be adaptable to multiple sensors and divergent logistic software packages used by shippers and carriers within the supply chain.

The final determination of what actual data are required by the user of a container security/monitoring system will depend on the user's own needs and the needs of the government into whose country the containerised shipment is sent.

Although the smart container market is just developing, there are significant entries into the market, including **Savi Technology, IBM, Motorola and GE/Siemens** (see *Cargo Security International*, December/January, page 38). Unfortunately, they provide little more than an electronic lock and global positioning system (GPS) tracking since they seem to rely heavily upon radio frequency identification (RFID) technology. Only a satellite system can provide in real time all the logistics/Customs data and sensory information indicated above.