http://www.maritime-executive.com/article/what-the-rotterdam-rules-should-do-for-global-supply-chain-security

The MARITIME EXECUTIVE
INTELLECTUAL CAPITAL FOR EXECUTIVES

What the Rotterdam Rules Should Do for Global Supply Chain Security

Thursday, March 31, 2011

By Dr. Giermanski, Chairman of Powers Global Holdings, Inc.

CURRENT U.S. SUPPLY CHAIN SECURITY PROGRAMS

At the present time we have a number of supply chain security programs. Of those programs, three stand out as particularly significant in the Department of Homeland Security (DHS) decision making, especially as it relates, but not limited to the maritime supply chain:
1. The Container Security Initiative (CSI);
2. Customs Trade Partnership Against Terrorism (C-TPAT); and
3. The Ten + Two Program.

1. Brief Discussion of Weaknesses in CSI, C-TPAT, and Ten + Two

a. The Container Security Initiative was announced as an initiative of U.S. Commissioner of Customs after Sept.11, 2001. It was codified into U.S. Law in the SAFE Port Act, signed October 13, 2006, and supports cooperative G8 action on transport security. Among its core purposes are the identification of high-risk containers (advance information and intelligence); prescreening and evaluation before sailing to the United States through the filing of the 24-hr manifest; X-ray and gamma ray screening; and the use of smarter, more secure containers.

CSI is consistent with WCO Framework of Standards to Secure and Facilitate Global Trade. *Section 1-2-4 of Standards* pronounced that supply chain security begins at stuffing (loading) the container and ends at unloading the container at destination. *Appendix 1 to Annex 1 of the Standards* is more specific by spelling out that continuous control from stuffing, through intermediate handling, loading on a carrier, off loading, terminal security, and unloading at destination are essential. Finally, the Standards require the electronic transmission of trade data

and the use of Edifact (Electronic Data Interchange For Administration, Commerce and Transport) and XML (Extensible Markup Language) as EDI (Electronic Data Interchange) protocols. In 2005, the United States adopted the WCO Standards, joining other Customs Administrations around the world who are members of the WCO and who believe that security begins at origin and ends at destination, managed with electronic documentation and communication.

Consistent with one of its purposes, CSI requires that all manifest information be electronically provided 24 hours before containers are laden into vessels at foreign ports destined for U.S. ports. Manifest data are generated by the shipper at origin. *At the present time, there are 58 operational ports participating in CSI.* Its weakness is in its core component: the 24-hour manifest. A manifest is like a tally sheet of what the vessel is carrying. For example, among the data are information such as numbers and quantities, commodity description and weight, and hazmat code. Except for visible cargo, the carrier has never known for sure what is in a locked and sealed container. This was recognized ever since we have had locked containers. The vessel carrier was forced to use honest terms like FAK (freight of all kinds) or STC (said to contain) which accurately explained that this or that was supposed to be in the container. The reality is no different today under the Container Security Initiative, except that the carrier is prohibited from using those phrases. The carrier must put on the manifest what the shipper or his agent says the contents are. In essence, nothing has really changed. However, the purpose of the CSI was to develop partnerships with foreign authorities to identify high-risk cargo containers originating at ports throughout the world before they are loaded on vessels destined for the United States. As an information-based system it depends on the vessel carrier's manifest to identify the cargo in a container that the vessel is carrying. Unfortunately, the carrier makes and files the manifest and, consequently, is *100% dependent* on the shipper (consignor) or the shipper's freight forwarder for accurate information about contents. As such, the vessel carrier serves as a third party in stating the contents of the container, the equivalent of hearsay.

Therefore, in CSI the details and accuracy of cargo information will always be linked to the person or firm that provides the cargo information to the vessel carrier who actually completes and files the 24-hr. manifest. The carrier has no first-hand knowledge of the container's contents. CSI's 24-hour rule places the responsibility of sending the manifest to *Customs and Border Protection (CBP)* with the shipping line, specifically the liner that loads the container into the vessel at the foreign port for movement to the United States. In reality, the carrier is still filing what the container is *"Said to Contain."* Only now, instead of using the term *"STC,"* the carrier will use the harmonized tariff number of the products furnished by the shipper or his agent. The vessel carrier still doesn't really know what is in the container.

b. Another CBP supply chain security program consistent with WCO Standards is *C-TPAT*. Its purpose is to increase security from the point of origin to the point of arrival. Specifically C-TPAT, a partnership program between the private sector and CBP, requires that security begins at stuffing with the recommendation for tracking, monitoring and breach detection systems. C-TPAT also mandates container inspection to be a seven-sided-process (sides, both ends/doors, ceiling/floor, undercarriage). Ultimately, however, it relies on the truth and accuracy of information provided. Not only the United States relies on accurate information. The *EU's AEO, Canada's PIP (Partners in Protection), Jordan's GLP (Golden List Program), and New*

Zealand's SES (Secure Export Scheme) are examples of other government programs, different, but generally consistent with the WCO (World Customs Organization) framework of standards. As recently as June 2010, *Korea's AEO* program was recognized as comparable to C-TPAT. Like C-TPAT, each needs verifiable information.

c. One of the latest CBP programs is the *Ten + Two Program.* This program requires the filing of 10 pieces of information by the U.S. importer on companies involved in an import shipment. If not filed, CBP could issue a "no load" order on the import. The additional 2 other pieces of information are for the carrier and include the vessel stow plan and container status message (information related to container arrival at port, location, stuffed or empty, etc.). Called *Import Security Filings (ISF),* they can be filed by either importers "or their agents." For a big importer who imports directly from the foreign manufacturer or distributor in full container loads, filing these elements accurately should be without difficulty. The requirement for use of the lowest bill of lading or house bill of lading can easily be met. When the motor carrier arrives to pick up the load at the shipper's location, it is provided to the carrier for signature at which time it becomes the contract for carriage to another location like a seaport where another maritime bill of lading is given by the vessel carrier. If not made by the shipper, the motor carrier makes the original bill of lading.

Although the information about the contents of the shipments is easily reportable and should be known to the U.S. importer, in fact, the importer only knows what he expects to be told: that the cargo is what he order, in the quantity he order, and on its way. Again, like in *CSI and C-TPAT,* the contents are really not known nor can any verification of contact be attributable to a particular person. Perhaps only on a LCL (less-than-container load) shipment where different shippers' and consignees' products are loaded together in the same container, the authorized consolidator who completes the stuffing of the container may know its contents. However, that also may be difficult because cargo in boxes is not visible. So what is the solution?

2. Impact of the Rotterdam Rules on CSI, C-TPAT, and Ten + Two

In September 2009, the United States became a signatory to the *United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (Rotterdam Rules).* When signed by the U.S. President with the "Advice and Consent" of the Senate, there could soon be a new day for shippers, consignees, and vessel carriers with respect to carriage of goods by sea. In the United States, the *1936 Carriage of Goods by Sea Act (COGSA) will be replaced by the Rotterdam Rules(Rules).* Also the Rules "…will supersede the Hague, Hague-Visby, and Hamburg Rules." The COGSA's "tackle to tackle" mode (where the period of time the goods laden into, and discharged from the vessel are the responsibility of the vessel carrier) disappears under the Rotterdam Rules. According to the U.N. General Assembly, the Rotterdam Rules is a ...uniform and modern global legal regime governing the rights and obligations of stakeholders in the maritime transport industry under a single contract for door-to-door carriage. *The U.N. General Assembly adopted the Rotterdam Rules on December 11, 2008.* On September 23, 2009 the *Rules were ratified by sixteen original signatories* (Congo, Denmark, France, Gabon, Ghana, Greece, Guinea, the Netherlands, Nigeria, Norway, Poland, Senegal, Spain, Switzerland, Togo and the United States) in a formal ceremony in Rotterdam. Today, a total of twenty countries have signed the Rules.

The new door-to-door liability instead of the tackle-to-tackle liability places the carrier directly in a virtual chain-of-custody regime. Now, *instead of the vessel carrier filing the 24-hour rule* based on what other supporting carriers said is in the container, *the vessel carrier will be automatically and actually responsible to know what is in the container.* The vessel carrier will have to use vetted motor carriers for direct shipper-carrier business and vetted forwarders and third-party logistics providers for indirect relationships between shipper and vessel carriers.

While a new world with respect to liability, it's also a new world for the requirement of electronic commerce. The heart of communications within the new Rules is electronic data flow and the value of electronically stored information, (ESI). The Rotterdam Rules allow and promote that all the data involved in the door-to-door movement be transmitted electronically. *Chapter 3, "Electronic Transport Records," contains Articles 8, 9, and 10. Article 8* specifically deals with the "Use and effect of electronic transport records.
(a) Anything that is to be in or on a transport document under this Convention may be recorded in an electronic transport record, provided the issuance and subsequent use of an electronic transport record is with the consent of the carrier and shipper; and **(b)** The issuance, exclusive control, or transfer of an electronic transport record has the same effect as the issuance, possession, or transfer of a transport document.

Article 9 sets forth procedures for the use of negotiable electronic transport records, and Article 10 treats the replacement of negotiable transport documents or negotiable electronic transport records. Article 10 further covers when the negotiable electronic document should be surrendered or replaced. This use of electronic data transmission is not only consistent guidelines from the *WCO Standards, the Kyoto Convention ICT Guidelines* to facilitate cross-border trade, and the *UN "Single Window"* adopted by the United States and exemplified in *CBP's "E-manifest" and ACE (Automated Commercial Environment)* usage, it fits nicely with some changes to the Federal Rules of Civil Procedure that took effect on December 1, 2006. *Rule 16, Rule 26, Rule 33, Rule 34, Rule 37, and Rule 45 were modified,* resulting in the principle that "electronically stored information," is a class of evidence and equal to paper or any other type of physical evidence. Each rule is distinct but related. *Rule 16* allows pre-trial meetings to discuss discovery issues regarding electronically stored information (ESI). *Rule 26* clarifies the need to disclose information about holders of ESI and its description before a discovery request, and allows the safeguarding of privileged information to be withheld or returned. *Rule 33* makes it clear that ESI includes business records. *Rule 34* defines computer-based and other digitally stored data as ESI and its format as a separate category and subject to production and discovery. *Rule 37* address the destruction of ESI, and when it can or cannot be destroyed. Probably, the strongest rule alteration is in *Rule 45*. It recognizes ESI as a distinct category of discoverable information allowing for subpoena of it in the same way as with paper documents. Subpoenas may also be executed on individuals or companies not directly involved in the litigation. ESI clearly includes electronic transport documents and records.

SUPPLY CHAIN SECURITY IN THE FUTURE
The change from port-to-port liability to origin-to-destination liability will make all vessel carriers review their liability exposure and begin to focus on security issues connected to it. Specifically, the new Rules should cause the following:
• *First,* their responsibility begins at the shipper's place of business, not at the port.

• *Second*, truck or rail bills of lading from the shipper's place of business to the port of debarkation will have to be validated as true. Therefore, the vessel carrier may finally know what's in the container making the vessel carrier's submission of CSI's 24-hr manifest more accurate by reflecting known data about contents for which the ocean carrier is responsible.
• *Third*, the ESI transmitted is subject to discovery and is usable for not only criminal, as it has been, but now also for civil matters. Accuracy then is paramount and records of the international movement must be maintained.
• *Finally*, the Rotterdam Rules should encourage vessel carriers to use some form of container security device (CSD) or suggest to their shipper-customers to use CSDs that will provide the identify of an accountable agent at stuffing who verifies cargo and quantity, potentially limiting or mitigating the vessel carriers legal responsibility and providing an increased degree of security to comply with government needs and mandates.

CONCLUSION

Even though the *United States is a signatory to the Rotterdam Rules,* for the Rules to take effect, they must be ratified by the *consent of the U.S. Senate and signature of the President.* In this case, the only potential objectors are likely to be the vessel carriers themselves. However, given that all of the major vessel carriers are foreign and in light of other nations agreeing with the Rules, it seems that adoption of them in the United States is not only appropriate but also compelling and hopefully inevitable. More than that, these Rules should have *a positive impact on this nation's security* by enhancing our existing supply chain security programs and by encouraging the use of container security systems that augment the Rules by verifying the cargo, tracking the container's movement, detecting and reporting unauthorized access and reporting any violation of the cargo movement's integrity. Therefore, for the sake of our security, and in contrast to other contention actions within the Senate, a positive vote for the Rotterdam Rules should be a welcome event for the nation. *That vote should be expedited.*

About Dr. Giermanski

Dr. Giermanski is the Chairman of Powers Global Holdings, Inc. and President of Powers International, LLC, an international transportation security company. He served as Regents Professor at Texas A&M International University, and as an adjunct graduate faculty member at the University of North Carolina at Charlotte. He was Director of Transportation and Logistics Studies, Center for the Study of Western Hemispheric Trade at Texas A&M International University.