

# Smart moves

*Jim Giermanski of Powers International argues that US government agencies need to reassess their approach to transshipment security*



Dr Jim Giermanski is Chairman of the Board of Powers International Inc., an international transportation security company.

Contact:  
Jim Giermanski  
Powers International Inc.  
Email: powersintnlinc@bellsouth.net

Several years ago, I wrote a short treatment focusing on the problems thrown up by the China Memorandum of Understanding (MoU) and the requirements of **Customs and Border Protection (CBP)** (*Textile World*, 17 October 2006). Essentially, China and the United States agreed to cooperate in enforcing certain levels of textile trade. Specifically, the United States had concerns about the issue of transshipment in that it could circumvent these levels and avoid appropriated taxes and thereby hurt the US producer of certain textile products. The MoU required, in addition to paper documentation, electronic transmissions of data directly to CBP to describe the shipment, country of origin, descriptions, quantities, etc.; all normal information required for a legal entry into the Customs' territory of the United States.

Earlier this year, I also wrote an article on the shortcomings of the *Container Security Initiative (CSI)* (*The Maritime Executive*, March/April 2009). More specifically, I pointed out that even if the electronic data transmitted 24 hours before the goods are laden into the vessel in a foreign port were true, there would still be a transshipment problem that has yet to be addressed by CBP.

We have, therefore, waited many years for a fix that apparently nobody in the **Department of Commerce (DOC)** or the **Department of Homeland Security (DHS)** has heard about, or knows about, or has seen. However, based on my direct knowledge, the rest of the trading world is considering or is in the process now of evaluating existing systems that can provide the solution to transshipments, specifically the European Union (EU), China, South Africa, South Korea, Pakistan, Malaysia, and Mexico. Therefore, one must necessarily ask why is it that the United States is not evaluating solutions to the transshipment

problem?

I have often been critical of the DHS and CBP and, in particular, about their leadership in the container security area. Take, for example, CBP's reliance on Radio Frequency Identification (RFID). RFID hasn't proved to be really workable in a global system. Its historical nature, divergent frequencies, protocols, problems of access to infrastructure for the placement of antennas in a land-locked system and its use as an improvised explosive device (IED) diminish its usage (see *Cargo Security International*, October/November 2009, page 44).

Or take, for example, CBP's selection of **General Electric (GE)** and its *Commerce Guard* system as the appropriate firm and technology to test RFID along the United States' southern border with Mexico. GE not only withdrew from the border test, it also appears to have dropped out of the container security business (perhaps because it could not sell enough of a system that many doubted could provide a solution to the global supply chain anyway). Not only did it drop out, but it also announced in April that it is to sell 81% of its Homeland Protection business to **Sagem Sécurité**, a division of the French aerospace and defence firm, **SAFRAN**.

Finally, the most important indictment of CBP's failure to solve the transshipment vulnerability issue is provided in this official statement: '...there is currently no proven technology which can address transshipped containers'. This statement was contained in the testimony on container security of Acting Customs and Border Protection Commissioner Jayson P. Ahern before the **House Appropriations Committee, Subcommittee on Homeland Security**, released on 1 April, 2009. In fairness, his use of proven technology may extricate him from an otherwise seemingly false statement.

Today, evaluations are currently underway of smart containers that do, in fact, solve the transshipment problem. Unfortunately, the United States appears to be unaware of that.

Smart containers can not only address the concern over unsupervised containers sitting at transshipment ports, but also their use can solve the issue of the China-US textile MOU. These containers can address the problem of transshipment vulnerability in the following ways:

A smart container is part of a system's approach necessary to coordinate all facets of the supply chain process to ensure visibility and security beginning at origin and ending at destination. The container records the identity of the person who supervised the stuffing and securing of the container at the foreign point of origin, a responsibility set forth in the **World Customs Organization (WCO)** standards and in the US *Customs Trade Partnership Against Terrorism (C-TPAT)* programme and the EU's *Authorised Economic Operator (AEO)* programme. It also records the identity of the person opening the container at the destination, providing a global origin-to-destination chain-of-custody

Smart containers also electronically capture trade data that will link to other documentation

Consistent with C-TPAT requirements to conduct a seven-point inspection of the container, a smart container is able to detect a breach anywhere within its body, not just through the doors

The smart container is able to report a breach in real time or close to real time with the date, time, and geographic location of the breach anywhere in the world, but especially at transshipment ports

The smart container can give its geographic position throughout the supply chain when queried, or automatically give its position if it is off its designated course of travel in controlled environments

Finally, the smart container is adaptable to different sensors and will be able to communicate with, or be adapted to, divergent logistic software packages used by shippers, carriers, and government Customs authorities.

CBP must first realise that it is lagging behind the rest of the world in container security evaluations and use. This may be because it is responding to political pressures in its decision making, but at the moment it seems to be failing to engage with the security and supply chain issues relating to containerised shipping within the global supply chain.

For the DOC, there is a solution that would avoid circumventions of the China-US MOU and would ease the onerous obligations put upon China to prove it has avoided circumventions. I would suggest, in cooperation with CBP, that it should contact appropriate US textile importers and engage its equivalent in China (that is already testing smart containers) to evaluate smart containers in shipping sensitive textile categories or products. I would suggest that DHS leadership execute three changes. First, approach the EU to discuss participation in the EU's Seventh Framework Programme which is designed to research and develop an ideal container security management system. Second, approach Mexico to develop a co-operative relationship involving smart containers. And third, ensure that knowledgeable leadership in the field of container security is in place within CBP.

Smart container use provides homeland security, enforces the agreed levels of textile imports from China, and can prevent circumvention of the agreed levels by transshipments or rerouting and the incidences of false declarations concerning country or place of origin. Finally, it reduces or eliminates falsification of official documents, deters commercial fraud, and ensures proper Customs duty collections. All of this is achievable now. Why the delay?

*'Today, evaluations are currently underway of smart containers that do, in fact, solve the transshipment problem. Unfortunately, the United States appears to be unaware of that'*