

Boxing clever

James Giermanski considers how the US Department of Homeland Security should change its focus to encourage the take-up of smart containers

The development of container security or smart box technology is, on the one hand, encouraged by the **Department of Homeland Security (DHS)**, and on the other seriously impeded by it. What can be done in developing and using smart box technology and what is being done are also on divergent paths.

Furthermore, the DHS's limited criteria for defining a smart container may even promote and encourage the development and implementation of inferior technological applications that appear to run contrary to the current global movement to switch, when possible, from preparing and sending hard-document information to transmitting electronic data. One must logically conclude that the DHS either knows what it wants to do but does not know how to achieve it, or it does not really know what it is to do about smart container technology. The latter seems to be the case.

Government's role

First, it is not the US government's role to develop container security technology. It is the government's role to determine the level of security it needs to cope with the potential security threats inherent in the millions of containers entering US ports. Second, what the DHS also could do is to set the highest level of security protection presently possible as the lowest level of acceptance. Third, its role is to evaluate all container security technology, not just the technology offered by those firms that can afford lobbyists, and afford to make significant contributions to political campaigns of those in the **US Congress** who can influence the DHS (although that appears to be difficult to do, given the size and complexity of the DHS bureaucracy).

The DHS should also not be inordinately influenced by powerful industry groups such as the **Retail Industry Leaders Association (RILA)**, which has been criticised for putting security second to the cost of security and the retailers' bottom line. Fourth, if the

'The government's role is to evaluate all container security technology, not just the technology offered by those firms that can afford lobbyists'

private sector is to develop smart box technology, it must realise some benefit for its efforts. Therefore, the DHS must reward the users of smart container technology with tangible benefits like 'green lanes' that exist at some land ports-of-entry, but not at seaports. Finally, the DHS must ensure that smart box technology protects more than just the door, and it must be consistent with the current and future use of electronic communication, tracking, and documenting.

Level of DHS sophistication

Smart box technology available now far exceeds the level of current requirements as envisioned by the DHS. Additionally, the specifications demanded by the DHS are substantively questionable as to their value and appropriateness. One need not look far to find an example. In the latest Request for Information (RFI), an information-gathering and planning vehicle used by the DHS in support of the **Customs and Border Protection (CBP)**, **Johns Hopkins University's Applied Physics Laboratory** (under contract with the DHS) sent a letter dated 8 November 2005 to potential vendors. The letter stated: 'The purpose of this request is to gather information to identify and evaluate available state-of-the-art container and trailer tracking devices suitable for in-bond shipments.' That statement, alone, poses two serious questions. What does the DHS believe is 'state-of-the-art', and why has it taken this long after 9/11 for the DHS to realise that the CBP had little or no knowledge of or control over containers

James Giermanski is the Chairman of cargo security specialist company, Powers International Inc.

coming into the US and moving throughout the US under bond. I will focus on 'state-of-the-art' issues. The in-bond question is worthy of separate treatment.

The level of 'state-of-the-art' for the DHS is the following:

Sensing

- The container and trailer security device must be able to electronically detect closing and opening of either door of the container/trailer. Monitoring the door status must be continuous from time of arming to disarming by authorised personnel.

- Optionally, the system should be able to provide near-continuous tracking of the location of the in-bond shipment while transiting through the US.

Alerting

- The device must monitor the sensors for conditions warranting a tamper alert.
- Provide notification of all alerts or change in status events.

Data

- The container and trailer security device must be able to record and maintain a digital file of all time-stamped alerts, armed/disarmed events, and other optional data such as container/trailer and device IDs.

It appears that the DHS wants a 'smart door'. The DHS says that a smart door must remember how many times it was opened and when it was armed and disarmed. Why, however, does the DHS not care about the other sides of the container or trailer? There is little trouble in making a surreptitious entry into a locked container while never disturbing the doors. Why is there no requirement to track the container? What about reporting in real time or as close as possible to real time the actual entry into the container? I asked these questions to the DHS directly a month before the RFI was released and got the following reply: 'We have to crawl before we can walk.' Protecting the doors is not



container security, nor does it qualify as smart-box technology. I have witnessed and directed breaches of both containers and trailers without disturbing the locked doors. Even the March 2005 requirements for US importers who are participants in the Customs-Trade Partnership Against Terrorism (C-TPAT) mandated a seven-sided inspection of a container: 'Front wall, left side, right side, floor, ceiling/roof, inside outside doors, and outside/undercarriage.' Here, the DHS is clearly suggesting that an unauthorised entry is not limited only through the doors. The DHS should have said not 'crawl' or even 'walk'. It should have said: 'We need to run.'

In my private meetings with the DHS, the agency has been adamant about sensors that can withstand the racking of containers during their voyage. In fact, a decision was made that any smart container device (for the DHS, this means door device), must still function if the container racks or opens by 40 millimetres (mm). The basis for that decision is again questionable to practitioners in the field. In a discussion in which I participated in September 2005, two vessel captains and a former

vessel carrier owner were amazed at the 40 mm criterion. They said any container that opened that much should not be used by shipping lines. In follow-on discussions in Europe, the same response was given by vessel professionals in Germany. Another DHS criterion is more realistic but still questionable. The DHS wants a 99% false/positive threshold – in other words, the device must not fail more than once in a 100 uses. This criterion may or may not be the right one. The scientific community uses different confidence levels for different purposes. Therefore, if one is using a smart container to thwart thefts and hijacking of cargo, or for supply chain tracking information, one would likely use a 95% confidence level. While the 99% false positive threshold is laudable, the requirement of obtaining near-perfection is extremely difficult in the global container market, and more importantly inhibits the development and implementation of new ideas and practices.

Not only are we faced with the movement towards the establishment of questionable standards, but also the conspicuous absence of movement

towards the establishment of criteria requiring the capacity to transmit electronically supply chain, trade, and CBP-related data. In June 2005, the 166 member countries of the **World Customs Organization (WCO)** – including the United States – unanimously adopted the final Framework of Standards to Secure and Facilitate Global Trade (see *Cargo Security International*, August/September, page 7). In the Customs-to-Customs Pillar of the document is the following statement: ‘Maintaining cargo and container integrity by facilitating the use of modern technology is also a vital component of this pillar.’ This statement is further defined as advance electronic information. In more specific detail, the WCO Framework calls for exporters or their agents ‘to submit an advance electronic export goods declaration to the Customs at export prior to the goods being loaded into the means of transport or into the container being used for their exportation.’

Deborah Spero, the Acting Commissioner of the US CBP, confirmed the importance of the WCO Standards in a recent press statement: ‘Adopted unanimously by the WCO Members in June 2005, the WCO Framework of Standards provides global standards for supply chain security for implementation by the public and private sector that will secure international trade supply chains and facilitate the movement of goods globally.’

In December 2005, the DHS announced that its Automated Commercial Environment (ACE) programme containing a secure data portal will come on line in 2006/2007. Since smart containers are able to communicate electronically from stuffing to destination and even carry trade data like that contained in the Inward Cargo Declaration, Customs Form 1302, why should this not be mandated? The DHS has no requirement to include this type of communication. Within my criticism of DHS in performing one of its core responsibilities, the obvious question

‘While the 99% false positive threshold is laudable, the requirement of obtaining near-perfection is extremely difficult and inhibits the development and implementation of new ideas and practices’

surfaces. Just what is a smart container?

Smart container

It seems there are no standards to define a smart box. In light of this, I think it is appropriate to focus on what a smart box should do. If there could be agreement on that, perhaps a definition would be more easily achievable. In my view and in the view of others, a smart container must perform at least seven clearly defined operations:

- A smart container must be a part of a system approach necessary to coordinate all facets of the supply chain process to insure visibility and security. That begins at origin. Therefore, the container must be able to record the identity of the person responsible for monitoring the ‘stuffing’ and securing of the container at the foreign point of origin.
- There should be an electronic capturing of certain trade data that will link to other documentation. Examples would be the container number, or booking number. One could even include portions of the Inward Cargo Declaration, Customs Form 1302.
- Consistent with C-TPAT requirements to conduct a seven-point inspection of the container, a smart box should be able to detect a breach anywhere into its body, not just through the doors.

- The container 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.
- The smart container is one that 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.
- The container must recognise and record the identity of the authorised person opening the container at destination.
- Finally, the container should be adaptable to different sensors and be able to communicate with or be adapted to divergent logistic software packages used by shippers and carriers within the supply chain.

Time to re-think

For me, a definition is obvious. A smart container or smart box is a system in which the container talks directly as needed and answers questions when queried. Its communications are both supply chain and security anchored. And it must be recognised and acknowledged that a smart container is not just a locked and monitored door. To do its job effectively, the DHS must recognise the existence and availability of advanced, more robust benefits of technologies that are already here. None of the attributes of the smart container that I suggested is somehow left for future development. Products are available today. The US government’s focus ought to be on encouraging the use of these applications by offering as many benefits as possible to the industry users of these technologies to impact positively on the users’ bottom line. Only when that happens, will our security level increase, better serving the US and all nations adopting similar standards.

Contact:
 James Giermanski
 Powers International
 Tel: +1 704 825 4741
 Email: powersintlinc@bellsouth.net