Container Security: Who's In Charge?

Guest columnist Jim Giermanski takes issue - actually seven specific issues - with DHS comments on the role of technology in container security.

By James Giermanski

May 06, 2008 —

On April 2, 2008, Deputy Commissioner, U.S. Customs and Border Protection (CBP), Jayson P. Ahern gave a statement at the Hearing before the Committee on Appropriations, Subcommittee on Homeland Security, U.S. House of Representatives. Although unremarkable in many ways, his conclusions regarding the Role of Technology as it applies to container security were extremely disturbing, and if these conclusions are representative of CBP, they give one the feeling that nobody in management at the Department of Homeland Security and especially at CPB knows what they are doing or talking about. If I'm right, we're in big trouble.

Statement 1
In what looks like an attempt to excuse CBP from indecision, Ahern said:

"It is important to note that there is no single technology solution to improving supply chain security."

Response
Of course there may not be a single technology. There's no single car, boat, aircraft, knife, or piece of cheese, but each do the job they are designed to do. Equally, for container security, there are many technologies that can provide solutions to improving supply chain security. For instance, satellite, RFID, Zigbee, and two cans and a long string are technologies. All but the two cans and a long string are used today in supply chain security around the world. Each has positive and negative qualities, but each serves in its way to improve supply chain security, just as different cars or knives do their job to accomplish their purpose. His statement seems to say that unless there is only a single technology, CBP cannot make a decision on technology and container security. How easy it would be never to have options!

Statement 2
"Priority should be given to effective security solutions that complement and improve the business process already in place, and which build a foundation for 21st century global trade."

Response
Where has Ahern's staff been, or what have they been reading, or do they read? We have research, opinion, and government statements already demonstrating what Ahern says it should do in complementing and improving business processes. Maybe I should start with the market itself. How can there be a market without systems and users?

Here's the market: Homeland Security Research Corp. says the container security market in 2009 will be more than $2 billion, rising to more than $4 billion by 2012.

Here's some research demonstrating the container security can improve and complement the global trade:
"Product safety 38% reduction in theft/loss/pilferage, 37% reduction in tampering;
"Inventory management 14% reduction in excess inventory, 12% increase in reported on-time delivery;
" Supply chain visibility 50% increase in access to supply chain data, 30% increase in timeliness of shipping information;
"Product handling 43% increase in automated handling of goods; and
"Process improvements 30% percent reduction in process deviations.
Here is some opinion on what cost saving there would be in facilitating the container's movement through Customs at our seaports:
"Estimates range from $600 to $700 per container per move (Bearing Point Study, 2003); and
"$1150 per move (AT Kearney Report, 2005).
And here is an official U.S. government statement regarding the savings gained from container security usage: 0.8 of one percent of value of contents of container (Congressional Budget Office, March 2006). So why doesn't CBP know this? Or does it, and is there another agenda?

Statement 3
"Because DHS does not believe that, at the present time, the necessary technology exists to adequately improve container security without significantly disrupting the flow of commerce, the Department did not make use of the rule-making authority or mandate the use of CSDs."

Response
In the first place, what DHS believes appears to be suspect. The real question is why does it believe what it believes? It is obvious that it doesn't know the technology, the market, or the value to the private sector in improving the global supply chain management. Now it believes that container security would disrupt the flow of commerce in face of the previously cited evidence. What is more amazing is that CBP is now, without the use of CSDs, disrupting the flow of commerce. Simply look at the time it takes to get though

CBP at our seaports. Look at the impact of the 24 hour rule under Container Security Initiative (CSI) that requires a carrier who doesn't know what's in a container, to send a manifest saying what's in the container to CBP 24 hours before the container is laden into the vessel. How long was that container at that foreign seaport? Then upon arrival at our seaports, there are the business-as-usual delays in clearing the import.
One of the fundamental purposes of the concept of Green Lanes, or Tier-3 treatment, was to facilitate and movement of cargo more quickly through our ports because the container was a smart container, the vary reason cited by Ahern that would disrupt the flow of commerce.

Statement 4
"It is important to note that CSD technology only improves container security if one can ensure the integrity of the shipment before the CSD is activated. Requiring such a device independent of a process to ensure that the goods within the container were secure before its application would have an adverse effect on security, creating the false impression that a dangerous shipment was secure."

Response
Obviously unknown to Ahern and his staff are container security systems that do just that. In 2002 when Powers International made its first container security system, we could identify and report the person who supervised the stuffing of the container at origin, detect and report breaches in a container, and identify the person who opened the container at destination. This technology was demonstrated successfully to the federal government under a contract with the U.S. Department of Energy at our biggest land port of entry, Laredo, Texas. Customs and Border Protection (CBP) was at that demonstration in 2003. The key to this system, of course, is the vetting of those who are allowed to supervise the stuffing of the container and arm the CSD. Container security devices and systems that do not have that exact system can likely authenticate the contents manually by using firms such as Cotecna that should be able to provide this service. Finally, if anything creates "&the false impression that a dangerous shipment was secure," it is the CSI 24-hour manifest submitted by the ocean carrier, and the pre-arrival data submitted electronically by third-party carriers on the southern border through a CBP portal of the ACE (Automated Commercial Environment) system. In the case of the 24-hour manifest rule, unless the ocean carrier built (loaded) the container itself, there is no way of knowing what's in the container that it receives from the shipper or maritime freight forwarder. In the case of pre-arrival data required on the Southern border, a drayage (transfer) motor carrier or more likely its approved carrier representative, who files the arrival data for them, is ignorant of the actual contents. The reason is that the drayage carrier picks up a sealed trailer in a drop lot ready for transfer to the United States, and its third party filer never even sees the trailer. CBP does not know what is in it either. Therefore, neither of these required submissions can prove a shipment is safe. Filing entry data when a northbound shipment arrives at the border without direct content verification at origin does not ensure the container or trailer is, in fact, safe.

Statement 5
"&following CBP's recent Request for Information on CSD technology, CBP will soon

be testing the CSD technology provided by the most qualified vendors who participated. If this technology passes the laboratory testing phase, the devices will then be tested in real world operational environments."

Response

Again, it appears that Ahern does not even know CBP's long history of its RFIs and the money already spent on CSDs. In 2005, (two years after a system doing what CBP needs was demonstrated in the field) CBP released a Request for Information (RFI), an information-gathering and planning vehicle used by DHS. DHS used Johns Hopkins University to manage the RFI. Johns Hopkins University's Applied Physics Laboratory released a letter dated November 8, 2005 for use by potential vendors. The letter stated in part, "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."

1. Sensing

a. 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 authorized personnel.

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

2. Alerting

a. The device must monitor the sensors for conditions warranting a tamper alert.

b. Provide notification of all alerts or change in status events.

3. Data

a. 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&.

Then, two years after the government, itself, demonstrated that there was more to a smart container than just a smart door container, DHS still wanted a "smart door." DHS said that a smart door must remember how many times it was opened and when it was armed and disarmed. I asked DHS directly a month before the RFI was released why only smart doors constitute a smart container. The reply was: "We have to crawl before we can walk." Unfortunately, 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 of U.S. 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."

Then in 2006, DHS engaged two firms to develop a smart container. L-3 was one of those companies. It shared a $5 million plan "&to develop fully integrated cargo container security device to ensure supply chain integrity, automatically detecting threats that no other sealed cargo screening technology can discover in real time, including human beings, unauthorized entries or container breaches." L-3 completed its work. To this date, no standards or decisions on what a smart container should be have been released by CBP or DHS.

Another RFI was released in December, 2007 that required an industry response in February 2008. Ahern references this RFI in his statement to Congress. The December RFI, like the one two years before, was still focusing on "doors only" despite the fact that CSDs have long ago passed that low level of security. They are also inconsistent with and lag behind the progress of the private sector in moving away from doors-only detection and reporting. Since demonstrated in 2003, the private sector already had affordable technology that begins "at-stuffing" with the verification of contents and identification of the verifier, "all-sides" detection of entry and satellite communication and control through to destination, including the identity of the authorized agent opening the container. In fact, the RFI to which Ahern is referring was protested by an industry group as going backwards: In order to be compliant with the subject RFI, virtually all manufacturers and designers would need essentially to abandon their advanced system designs in lieu of what may be viewed in many cases as less capable technology and weaker designs. It went on to say: The specification of a single-purpose security device - managing door status only - severely limits the value of a CSD and increase vulnerability for undetected intrusion into the container. This is viewed by the CSDIA as a restricted and inferior security application, and as a cost that will only support compliance (ultimately) with a Government mandate. Other offerings, available today from a number of vendors, provide advanced technology that monitors cargo condition, location, status of discrete and high value packages virtually anywhere in the world.
In other words, CBP has been spending money appropriated to it in testing CSD technology since 2005 and is still at the "laboratory" stage, obviously still crawling. Why? One answer could be that it simply does not know what is already available, or what is already available is not from the favored companies, potentially linked to the Administration, or its leadership is intellectually challenged and virtually incompetent.

Statement 6
"The 9/11 Act amended the Safe Port Act by establishing that if an interim final rule was not issued by the Secretary of DHS by April 1, 2008, all containers in transit to the U.S. would be required to be secured by a bolt seal by October 15, 2008. DHS does not anticipate that an interim final rule will be issued by the April deadline. Therefore, effective 10/15/08, all containers will be required to be secured with the standard bolt seal."

Response
On June 24, 2005 all member countries of the World Customs Organization (including the United States) unanimously adopted the final Framework of Standards to Secure and Facilitate Global Trade. 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 (my emphasis added). 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 former Acting Commissioner of the U.S. Customs and Border Protection, confirmed the importance of the WCO Standards in one of her press releases.

"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."
Finally, in 2006 the Congress passed and the President signed the SAFE Port Act. In it, Congress defined a container security device: The term "container security device" means a device or system, designed at the minimum, to identify positively a container, to detect and record the unauthorized intrusion of a container, and to secure a container against tampering throughout the supply chain.
But in 2007, we saw a continuation of DHS and CBP's apparent ignorance of and even in-house division on container security. In January 2007, W. Ralph Basham, CBP Commissioner, stated I'm saying that just because you have a device that secures the doors does not mean that the container is secure. It just means that the doors are secure and not the whole container. If technology is being developed it should be toward making sure the entire container is tamper proof. That is the challenge. Not just the doors on the container but the entire container&. But, on December 18, 2007, as posted in American Shippers NewsWire, Basham's boss Homeland Security Secretary Michael Chertoff went to the other extreme by saying Therefore, effective Oct. 15, 2008, we expect to have the requirement in place mandating that all containers be secured with a standard bolt seal. In other words, contrary to the leadership of CBP who publicly announced the need for total container protection, and contrary to the mandate of Congress which said the Secretary shall issue a rule, and almost 6 months before the deadline to do so, and having already spent millions of dollars to develop a CSD, Secretary Chertoff decided that container security amounted to "dead-bolting" (my words) the container doors.

Statement 7
In discussing the need for issuing another RFI, this time for technology involving "crane-mounted" radiation detection technology to use at seaports to detect shielded radiation, Ahern said:
"The reliability, ruggedness, and standard operating procedures associated with this technology will not be extensively evaluated during these tests as field validation activity would be the logical course of action after testing with surrogates and actual threat material, but this requires more time."

Response
The problem is that these so-called crane-mounted scanners cannot detect shielded radiation at this time, and it will take years to develop them. Congress knew that the technology did not exist when the legislation was drafted. In referencing the requirement to scan at foreign ports, the 9/11 Commission Act of 2007 reflects the following with respect to its application:
...shall apply with respect to containers loaded on a vessel in a foreign country on or after the earlier of--(A) July 1, 2012; or (B) such other date as may be established by the Secretary under paragraph (3). (Section 1701)
Therefore, Congress is expecting that new portal machines, or in Ahern's statement, crane-mounted machines, will be developed and commercialized to detect dangerous radiation. The GAO -- in April of 2007 (GAO-07-347R, Combat Nuclear Smuggling) --

stated very clearly that the Domestic Nuclear Detection Office (DNDO) established and responsible for ASP development has not even collected all the testing data on its basic PVT portal detectors and is not close to any developed ASP portal detector. Experts do not expect a commercial version of the ASP anytime soon, if ever. We do not have the machines now, and we won't likely have them in 5 years (in 2012) as indicated by Congress. Therefore, Congress allowed for an extension until such time that these radiation portal detection machines become available.

However, the physics of detection are fairly simple. Gamma rays and neutrons from shielded HEU are detectable at only short distances and only when there is adequate time to count a sufficient number of detected particles. Five basic issues are relevant: the mass of the HEU core, the degree of shielding, the size of the radiation detector, the distance to the source, and the time necessary to integrate photon counts. Therefore, the closer a detector is to the source of emission and the longer it "sniffs," the greater the probability of detecting HEU. So the natural question is: does CBP know this and has it actually read the 9-11 Bill? Why is there an intention of developing crane-mounted scanning that cannot detect shielded uranium any time soon, when there are in-container systems that can detect it now?

They say we need to develop CSDs when they already exist. They say we need to develop portal and crane-mounted scanners to detect shielded enriched uranium when this detection capability already exists for use in containers. They say that doors are what is really important and are satisfied with bolting them when surreptitious container intrusions are not made through the doors. They say that CSDs will disrupt a flow, when CBP's current "layered" approach actually disrupts the flow of commerce. They say they don't know about any industry CSDs when there is a global market with U.S. entrants like IBM, Lockheed Martin, GE, Motorola, GlobalTrac, and Powers International with others like Raytheon considering entry. Then we have Astrium, Siemens, and Zoca in the EU, one of which is producing its product which includes a U.S. patent.

Only a few conclusions are plausible. One, CBP really does not know what is going on in container security worldwide. Two, it knows but has an agenda of working with certain companies that yet do not have the "origin-to-destination" system, along with detection and reporting capability worldwide. Three, its management may simply be lethargic and virtually dull, or fourth, it may not think container security is really a security threat and that the laws passed requiring performance do not really apply to them.

As a private citizen, not politically connected to either party, it is apparent to me that Congress cannot or will not do what we expect it to do. Who is in-charge of the nation's security—Congress, DHS, CBP, or the private sector? When this question can be answered, and safeguards are mandated, we should all feel safer. ##

Dr. James Giermanski is chairman of transportation security company Powers International and Director of the Centre for Global Commerce at Belmont Abbey College.