CSO
csoonline.com

Web Exclusives

DHS Decision-Making: Competence or Character?

Guest columnist Dr. James Giermanski looks at container security and argues that the Department of Homeland Security suffers from "seriously flawed decision-making".

By Dr. James Giermanski

Recently I met with a small group of former FBI agents at a monthly breakfast. The conversations, usually connected to past Bureau activities, moved to the discussion and criticism of Department of Homeland Security (DHS) and Customs and Border Protection (CBP). The flavor of comments follow: they're out of touch with industry in the container security area; they're in the pocket of big business; they lack vision; they're arrogant; and they don't have leadership; they lack talent; and more. However, while some old crusty ex-agents said it was "all of the above," the consensus, if there was one, was that the fundamental problem within the Department was weak and sometimes flawed leadership. While I would expect those comments about DHS from a competitive agency, thinking about the breakfast discussion later that day, it occurred to me that, perhaps, this really is a core problem, especially with container security. Therefore, I put together three examples of what I believe represents seriously flawed decision-making important to our security and reflective of questionable and inept leadership within the Department.

All examples involve decision-making tied to container security. The first example involves leadership incongruence within DHS as demonstrated by CBP's focus on and fascination with the electronic sensing of "doors only" access or entry into a sealed container. The second is the commitment to radio frequency (RF) devices for container security such as either RFID (Radio Frequency Identification) tags already in use at our ports, or according to CBP's Request for Information (RFI) dated December 12, 2007, the potential use of Bluetooth-related technology using prescribed frequency ranges published and available through the Federal Communications Commission (FCC). The third example is CBP's incredible reliance on import security programs with their inherent core concern for "inbound" container security to the exclusion of "export" container security. Only short examples of each of these three fixations will or should

demonstrate the level of competent leadership within DHS, perhaps making credible the talk around the former agents' breakfast table.

1. Doors Only

For some time now, when treating conveyance security devices, both DHS and CBP have focused on only doors. First, in November 2005, a Request for Information (RFI), an information-gathering and planning vehicle used by DHS in support of Customs and Border Protection, Johns Hopkins University's Applied Physics Laboratory on behalf of DHS 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." The level of sophistication needed and stated in the RFI seems clear.

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.

However, in January 2007 as reported in SecurityInfoWatch.com, 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, 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." Or, in my words, let's just bolt the doors.

However, one week before Chertoff's deadbolt-the-doors statement, CBP released an RFI on its Conveyance Security Device (CSD) requirements. This RFI, like the one two years before, is still focusing on "doors only" in spite of Commissioner Basham's statement on the need to secure the whole container. It is also interesting to note that the new 2007 RFI is still referencing the old "in-bond" shipment problem known to it and acknowledged in 2005, essentially admitting that for two years it has failed to address the in-bond issue and does not know if in-bond shipments were accessed during their travel through the United States, or for that matter what's really in the in-bond container. In the face of fairly clear direction contained in the SAFE Port Act of 2006, DHS and CBP failed to move at the pace specified in the law with respect to container security.

They are also inconsistent with and lag behind the progress of the private sector in moving away from doors-only detection and reporting. The private sector already has 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. One such system was demonstrated between Bremerhaven, Germany and Port Everglades, Florida in December 2006. [See Rick Eyerdam, Cargo Insecurity:

Locals Offer a Better Mouse Trap, Florida Shipper, May 28, 2007, pp. 7, 9, 76.] Although the Germany-U.S. pilot was for demonstration purpose, in reality the system actually caught thieves stealing from one of the containers and it located one of the containers unintentionally lost in transit. DHS is so far behind industry in container security that its decision-making in this area is anything but confidence-producing.

2. RFI of December 2007

Another amazing example of security knowledge and leadership, or lack hereof, is the new RFI. The RFI's synopsis reveals that "The primary purpose of the CSD System is to monitor the rear doors of a conveyance for an intrusion into the cargo space while in transit." While contravening Commissioner Basham's own statement on the inadequacy of doors-only container security, the real perilous point of this RFI is its calling for radio frequency technology, specifically cellular, and Bluetooth applications. Seriously considering these applications is not only foolish, but also dangerous, again putting into question CBP's knowledge of what constitutes smart box security. The use of almost any Radio Frequency (RF) applications to container security becomes, in effect, an Improvised Explosive Device (IED) if the container carries a bomb. The RF signal can trigger that bomb when that container arrives at one of our ports. The only difference between this IED and those used by terrorists, is that our own U.S. personnel "pull the trigger" causing the explosion!

On November 13, 2007 a small team of private and public sector scientists along with security and bomb experts performed a controlled blast in a container at a municipal bomb range. At the range, a detonator and a small amount of explosives were placed in the container. A transceiver, like the ones used by our CBP and DOD and operating on frequencies mandated by the Federal Communications Commission (FCC), sent a normal signal interrogating the container as is done everyday at our ports. The explosives in the container detonated. In simple terms, there is now scientific evidence that the use of RFID technology approved for container security and employed today by CBP at all of our seaports and land ports-of-entry can be used as an IED trigger, an indisputable fact unknown to CBP.

What was exceptionally relevant in this demonstration was that it showed that encrypting data as required in CBP's new RFI would not prevent the triggering of the explosives. Of course, maybe CBP doesn't know this either. If it did know, one would assume it would immediately stop RFID usage at our ports until a fix to the vulnerability was found. The truth has to be that CBP's leadership is uninformed. But this begs the question: how is that possible? The following may explain the ignorance factor. CBP, DHS, the Office of the Secretary of Defense (OSD), the Government Accountability Office (GAO), the Coast Guard, multiple port authorities, and congressional offices were invited to witness the demo. CBP was not only invited in writing but also by telephone. CBP, DHS, GAO, Coast Guard, and the port authorities refused to attend. One congressional office and specifically relevant and important OSD personnel did attend. As a result, OSD stated that the demo was valid and confirmed the findings that current RF signals used today can act as an IED trigger. Additionally, because of the poignancy of this demonstration, a follow-up meeting of Congressional staff, private sector security, and scientific experts

was called by a U.S. Congressional Representative for the first week of January, 2008 to address this vulnerability. CBP is also unlikely to be present at this meeting. Yet, in the face of known risks, CBP is continuing to use RFID at our ports, demonstrating its ignorance of this vulnerability or its lack of concern over it.

3. CBP Programs and U.S. Exports

The third problem demonstrating the leadership level of CBP and DHS is its lack of focus on the security vulnerability to our ports of cargo leaving the United States. Each of CBP's four major container security programs, the Container Security Initiative (CSI); Customs Trade Partnership Against Terrorism (C-TPAT); the Secure Freight Initiative (SFI); and the Non Intrusive Inspection (NII) has one focus: inbound cargo and equipment. (The following descriptions are based directly on official DHS and C-TPAT documentation.) So far, the CSI involves up to 58 foreign seaports where CBP has a presence. Its major instrument is the 24-hour rule that requires the shipping manifest containing logistics information to be transmitted to CBP in the United States 24 hours before the cargo is loaded at the foreign port into the vessel destined for the United States.

The SFI is a joint effort by DHS and the Department of Energy (DOE) designed …to scan containers for nuclear and radiological materials overseas and to better assess the risk of inbound containers. Announced in 2006, the program was implemented in 2007 in 6 foreign ports to gather information on potential carriage of nuclear material and report the information found. This data will be combined with other available risk assessment information such as currently required manifest submissions, to improve risk analysis, targeting and scrutiny of high-risk containers overseas.

The NII is smaller in scale and takes place at U.S. ports of entry directed at individuals coming into the country. The goal of the CBP Non-Intrusive Inspection Systems Program (Small Scale) is to match the technology and equipment with the conditions and requirements at ports of entry and Border Patrol checkpoints based upon a requirements analysis of the individual conditions at each location. The program uses hand-held equipment to inspect small-targeted cargo, parcels, luggage, and individuals, allowing system operators to examine their contents without the need for an intrusive manual search.

Finally, C-TPAT is a cooperative voluntary program between industry and CBP. Its purpose is to strengthen the entire global supply chain by requiring its volunteer firms to meet minimum security standards established by CBP. It is an "inbound" program, easily recognized as such by both its security mandates and the type of business participants permitted in the program:

U.S. Importers of record;
U.S./Canada Highway Carriers;
U.S./Mexico Highway Carriers;
Rail Carriers;
Sea Carriers;
Air Carriers;
U.S. Marine Port Authority/Terminal Operators;

U.S. Air Freight Consolidators, Ocean Transportation Intermediaries and Non-Vessel Operating Common Carriers (NVOCC);
Mexican and Canadian Manufacturers;
Certain Invited Foreign Manufacturers; and
Licensed U.S. Customs Brokers.

Because the primary focus of C-TPAT is imports, it has become the critical obstacle preventing recognition of C-TPAT as equivalent to the EU's counterpart, the Authorized Economic Operator (AEO), scheduled to be implemented in January, 2008. The lack of the inclusion of exports in the U.S. programs, specifically in C-TPAT, makes mutual recognition doubtful. So why does the U.S. leave out exports? Do exports serve as a potential host for terrorism? Is it any easier for a container bomb to take out a port and its nearby population going outbound from the United States? The answer is: it is no more difficult and is likely easier. However, unlike the European Union, CBP does nothing in its security programs to face that threat. During the preparation of the recent November 13th demonstration of RFID usage in seaports and land ports, a component of the team that concentrated on port vulnerability discovered that there is equal if not greater vulnerability from an outbound shipment. So why does CBP not include the outbound export function within its programs? Hopefully, the answer must be that CBP knows more than private sector security experts because if it does not, the competence of its leadership should again be questioned, especially with respect to container and port security.

I do not hold allegiance to either particular political party and do not like to present one side or the other in an analysis that should be as objective as possible. However, it appears to me that Representative Bennie Thompson, Chairman of the House Homeland Security Committee, was right on target in expressing his displeasure with the progress and efficacy of DHS with respect to complying with the SAFE Port Act, and with DHS' knowledge about comprehensive smart container systems that do more than check door integrity. In his press release Congressman Thompson said "The department is looked to for setting security standards and enforcing laws, and here they are doing just the opposite. This is the second time DHS is missing the mark on cargo security and it is two times too many. We shouldn't be waiting any longer for DHS to set standards for equipment that already exists."

Door-only, RF-only, and inbound-only are just three examples of "missing the mark." What does DHS say when a dirty bomb detonates in one of our ports because of action DHS did not take? For this writer, the depth and breadth of DHS knowledge of container security vulnerabilities that face us every hour constitute more than virtual misfeasance. It may demonstrate a lack of moral judgment that today puts not only our ports and their surrounding communities in danger, but also our entire economy including you, the reader. Maybe it should have been the moral character of DHS that we former agents ought to have been discussing at our breakfast table.

With respect to DHS and CBP, all of us deserve better.

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