

A Report Card on DHS Security Policies, Standards and Programs

“...there is currently no proven technology which can address transshipped containers...”¹

Jason P. Ahern, Acting Commissioner, Customs and Border Protection

Although the introductory quotation of J. Ahern represents just one issue of this country’s treatment of container security, it is based on the standards against which Ahern and others in DHS form their conclusions. It is not the issue of only standards that influence their decisions, laws and policies are equally important. In the case of container security, Ahern’s statement demonstrates the lack of knowledge of container and cargo security technology and practice that relates directly back to standards established by DHS. If one looks seriously at the claimed standards of technology and/or practices of Congress, the Department of Homeland Security (DHS), and Customs and Border Protection (CBP) in the global container and cargo security arena, it becomes obvious that the standards and practices to which they adhere are either unsupportable scientifically, or practically, or at best, weak in light of standards in the rest of the world. Of course, this is easy to say. Therefore, to be reasonable, honest, and convincing, it is necessary to treat with specificity examples of laws, standards, programs or practices of Congress, CBP or DHS. My analysis will examine only eight standards or criteria against which security decisions are made:

¹ Jayson P. Ahern, U.S. Customs and Border Protection (CBP), Testimony before the House Appropriations Committee, Subcommittee on Homeland Security, on Cargo and Container Security, released April 1, 2009

1. CBP's False Positive Standard;
2. Legislation on 100% Scanning;
3. CBP's Container Management Standard;
4. CSI and The 24-hours Manifest;
5. Sealed-Door Standard;
6. RFID Standard;
7. In-bonds standard; and the
8. Science and Technology Directorate CSD standard.

1. False-Positive Standard²

Whether this one is DHS's or CBP's, it really doesn't make much sense in practical terms and goes against any serious scientific appraisal. In 2005 and then in 2006, DHS determined that any smart container used for entry into the United States must meet a 99% false positive standard, that is, once in 100 times a smart container is permitted to alert a need to examine that is false, that is, when it is examined, all is normal – in other words, an alert that was false and unnecessary. That means, of course, DHS assumes that the other 99 times that it didn't alert, it was correct and there was no problem that caused the transmission of an alert signal. The smart container was then 99% accurate. However scientifically, while this standard may be applicable in laboratories where all conditions can be controlled, outside the lab in real-world conditions which cannot be controlled, it is impossible to achieve. For instance, we all want and are willing to pay for a 100% guarantee that when we take off in an airliner, we land without incident. But reality is that getting to destination and landing without incidents is not 100% assured.

The scientific community uses different confidence levels for different purposes. Therefore, if we are using a smart container to thwart thefts and hijacking of cargo or for supply chain tracking information, we would likely use and be happy with a 95% confidence level typically used in scientific research. While the 99% false positive threshold is laudable, the requirement of obtaining near-perfection is extremely difficult in the global container market and, more important, inhibits the development and implementation of new ideas and practices. So what do we do in the health care area? We look around to find a test, an indicator of potential risk, and a drug that can give us the best protection we can find. If our

² For an expanded treatment of this issue see: Dr. James Giermanski and Dr. Peter Lodge, *The Problem of Errors, DHS and the 'False Positive' Standard*, **Journal of Homeland Security**, October 2007

potential disease is cancer and we can find a drug that works only 80% of the time, should we not take it? Yes, it costs money, and yes, it is not a 100% sure thing, and yes, it may be uncomfortable to take. If an 80% false/positive was used in the container security area, Customs and Border Protection probably wouldn't like it. It may cost them, inconvenience them, and even slow down port clearance. So does that mean we don't accept it? We certainly can inconvenience some Customs and Border Protection employees whose salaries we pay.

Another concept to consider is the "reasonable man theory" commonly used in judicial or quasi-judicial proceedings. What would a reasonable man believe or do? Said another way, it's the 75% level of probability, or "probable cause." The grand jury system is based on it, and people's lives are affected by it, and the nation accepts it. Would it not be "reasonable" to have a minimum 75% standard of reliability instead of 99%?

It seems that a reasonable standard should allow a failure rate that still gives us the best protection possible. We are dealing with creative, dangerous persons against whom we must have the best defense attainable, not the best defense possible. We cannot afford to have no defense because of a bureaucratic standard that simply cannot be met with our current and likely future technology or cannot be developed because of unacceptable costs of added redundancies for sensors and communications. Containers are victims of our climates, temperatures, rough handling, rough roads, and rough seas. Perfect mechanical and electronic functioning of container security systems capable of all that is expected of them is unattainable at this time. The obvious conclusion is that the current False-Positive Standard is unrealistic and fundamentally flawed.

2. Legislation on 100 % Scanning

Congress legislated 100 % scanning and the president signed the legislation. The requirements to scan containers were contained in the *SAFE Port Act* signed into law in October 2006, and in the *Implementing Recommendations of the 9/11 Commission Act of 2007*, signed into law in August 2007. The *SAFE Port Act* says this about scanning at U.S. seaports: "*SCANNING CONTAINERS.-Subject to section 1318 of title 19, United States Code, not later than December 31, 2007, all containers entering the United States through the 22 ports through which the greatest volume of containers enter the United States by vessel shall be scanned for radiation. To the extent practicable, the Secretary shall deploy next generation radiation detection technology.*" (Section 121).

The new *Implementing Regulations of the 9/11 Commission Act of 2007* goes further by amending the *SAFE Port Act* to say:

"IN GENERAL.-A container that was loaded on a vessel in a foreign port shall not enter the United States (either directly or via a foreign port) unless the container was scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel also mandate scanning." (Section 1701)

The standard Congress is using is this: the United States can mandate that other sovereign states obey our law. How can we as a nation, mandate other nations to provide the means for or perform the scanning of containers inbound to the United States in their ports? There is a clear question of sovereignty and a foreign nation's right to decide what steps to take within its sovereign territory. The EU's Taxation Commissioner, Laszlo Kovacs said 100% scanning would not only not improve security but cost EU exporters. Further, even introducing U.S. legislation of this type puts the resource burden of protecting the United States on its trading partners (International Herald Tribune, Aug. 2, 2007). The UE commission is already examining whether these U.S. laws breach World Trade Organization (WTO) and World Customs Organization (WCO) rules (FT.com Europe, August 2007). Even Ralph Basham, the U.S. Commissioner of Customs and Border Protection (CBP) said on July 11, 2007, in a speech to the Center for Strategic and International Studies, that 100% scanning is "fundamentally flawed" and "just does not make sense" because it would impede the flow of commerce. Supporting commissioner Basham's position are Christopher Koch, president of the World Shipping Council (WSC), and Janet F. Kavinoky, Director of Transportation Infrastructure for the U.S. Chamber of Commerce (Florida Shipper, August 27, 2007). As recently as April 2009, Acting Commissioner of CBP Ahern affirmed that the U.S. cannot simply compel other nations to scan containers for us. He testified: *"CBP is currently taking a close look at what will be possible and useful and will come back to the Congress soon with a clear path forward."*

Of course, if this standard is sound, then other nations can mandate the United States to scan all containers leaving from the United States to their countries. If that happened, the U.S. could not scan all the containers and would likely refuse to do so. Therefore, the standard established by Congress is unworkable, unfair, and like the false-positive standard, flawed.

3. CBP's Container Management Standard

This standard is perhaps the most difficult to recognize since it seems to be simply compliance with Federal Law. If the law says to do something, DHS and/or CBP attempts to do so. The U.S. has numerous programs, some codified in law, that form what some might call the management standard. Specifically, the U.S. has C-TPAT (Customs Trade Partnership Against Terrorism), CSI (Container Security Initiative), the *10 Plus 2* program, and now from TSA (Transportation Security Administration), the Certified Cargo Screening Program (CCSP). However, an amalgam of disparate programs and models do not constitute a standard. The rest of the world has developed a standard to secure international trade, *ISO 28000*. ISO is the International Standards Organization.

*ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards...a network of the national standards institutes of 161 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organization that forms a bridge between the public and private sectors. Therefore, ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society.*³

Some of the international security programs like the U.S.' C-TPAT and CCSP, 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 government programs, different, but generally consistent with the WCO (World Customs Organization) framework of standards. The World Customs Organization released its *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 and XML as EDI protocols. Also 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

³ *About ISO*, <http://www.iso.org/iso/about.htm>

security begins at origin and ends at destination, managed with electronic documentation and communication.⁴

All represent, although unique in certain ways, some level of standardization of global cargo and container security. Yet, other than *ISO 28000* there is no single standard, and government programs vary. The European Union is attempting to develop a container security management system even though the EU has the AEO program. The EU's research program is entitled the *Seventh Framework Programme (FP7)*. The *FP7* is an EU-level program of the European Commission designed to bundle all research-related EU initiatives together under a common roof, playing a crucial role in reaching the goals of growth, competitiveness and employment through research involving global door-to-door container transport management, using ubiquitous track & trace technologies. The research will be done by the Smart Container Supply Chain Management (SMART-CM) Consortium. Its purpose to develop a service platform capable of

1. A single window approach, to achieve interoperability of Container Security Technologies;
2. Handling of events within the container transport chain, to enable minimization of processes' duration & cost and improvement of chain planning;
3. Continuous control of containers, to accomplish high level chain security;
4. Efficient exchange of information among the industrial actors and between industry and the customs authorities, based on authorization policies, to increase supply chain visibility; and
5. Working with existing initiatives such as that of AEO the U.S. Green Lanes implementation, to achieve faster throughput in transport corridors.

It should be noted that the U.S. has not been invited to participate, nor has interest been shown by the United States in participating. Thus, the United States really follows no global or single U.S. cargo or container security standard, and its security programs have obvious gaps in them. For instance, while international standards and models of cargo security embodied in *ISO 28000* and the WCO Standards hold that security begins at origin and ends at destination with equal concern placed on outbound and inbound containers, DHS models only look at inbound containers. Inbounds-only is shorted sighted and

⁴ For a comprehensive treatment of the development of container security standards see: Dr. Jim Giermanski, *The Development and Globalization of Container Security*, **Defense Transportation Journal**, September 2008, Vol. 64, No. 5, pp 16-22.

dangerous. In effect, it portends a “no risk” condition with respect to outbound containers.

Other nations are doing more. South Korea is modeling its program after the EU’s Authorized Economic Operators program. China is emulating the EU’s traceability guidelines, in both international and domestic in-transit movement of containers. Mexico is considering the equivalent of a certified C-TPAT. One can see that, in fact, U.S. models are or will be significantly weak in comparison as these nations institute their models and standards.

4. CSI and The 24-hours Manifest⁵

The Container Security Initiative or CSI (now codified by the U.S. *SAFE Port Act*) is a variation of the security programs like C-TPAT, or AEO. It is as weak as the false/positive standard used by CBP. Its weakness is in its core component: the 24-hour manifest. A manifest is like a tally sheet of what the vessel is carrying. 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 cannot use 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 Container Security Initiative 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. It is an information-based system that depends on the vessel carrier’s manifest to identify the cargo in a container that the vessel is carrying. CBP says *"It is critically important that Customs officers receive this information as soon as possible in the process...U.S. Customs officers need timely and accurate manifest data and they need it now."*⁶ 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 verifying the contents of the container, the equivalent of hearsay.

⁵ For an expanded treatment, see Dr. Jim Giermanski, *So You Think CSI works: Gummy Bears or Cocaine*, **The Maritime Executive**, March/April 2009, pp. 38-42.

⁶ http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/legacy/2002/82002/08072002.xml

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 carrier who actually completes the 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 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. The CBP mandate is that beginning in December 2002 carriers and/or automated NVOCC's (Non Vessel Operating Common Carrier) have to submit a cargo declaration 24 hours before cargo is laden aboard the vessel at a foreign port for any vessel beginning the voyage on or after Dec. 2, 2002. Originally, there were 14 types of data placed on the manifest; today there are 21.

While there are new data to report, nothing has really changed. For example, among the data are information such as numbers and quantities, commodity description and weight, and hazmat code. 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. We still don't really know what is in the container.

5. Sealed-Door Standard

Perhaps, the dumbest policy, model, or standard of all is the sealed-door standard. No scientific or empirical data are necessary to demonstrate its weakness. It was the outcome of DHS' inability to develop an alternative. 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.*

The former Commissioner of CBP, Ralph Basham, diverged from his predecessor and said in 2007 that “... any device developed to monitor the security of a shipping container must be able to detect unauthorized intrusions anywhere on the container, not just through the doors, to be part of a layered defense strategy in securing the global supply chain....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.”⁷ But, in the same year on December 18, 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.* Or, in my words, let’s just bolt the doors. And, 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 CBP has failed to address the in-bond security issue, therefore, ignorant of how many in-bond shipments were accessed during their travel through the United States, or for that matter what was really in placed the in-bond containers at their foreign origin. 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

⁷ Calvin Biesecker, *CBP Chief Wants Total Container Security Device*, **Defense Daily International**, January 3rd, 2007 11:56 AM EDT

Port Everglades, Florida in December 2006.⁸ 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.⁹

Two important observations must be addressed here. First, CBP acknowledges that the doors-only concept is flawed and unworkable. Second, CBP acknowledges that it is ignorant of existing security systems that detect and report access to any part of the container, including doors! The conclusion: Doors-Only, while still our standard, is fatally flawed and constitutes a vulnerability still not addressed!

6. **The RFID Standard^{10, 11, 12}**

It seems that RFID – the short term used to refer to radio frequency identification – has become the current “buzz word” among some of the largest retailers and importers in the country. Wal-Mart and Target are just two of the giants discussed in the literature. Recently, an A. T. Kearney report entitled **Smart Boxes**¹³ lauded the potential and actual use of RFID for certain supply chain applications. However, the application of RFID to container security and port security is less laudable, less effective, more costly, and certainly questionable as a primary means of international transportation security for containers. RFID applications, whether active or passive,¹⁴ have very clear weaknesses and impediments to usage in a worldwide context. The impediments are these: the absence of agreement on RFID worldwide standards; its land-based character and historical nature; its acquisition rights to real property for antenna placement, its cost, control, and maintenance of fixed antennas and related infrastructure; divergent world frequencies; and divergent RF (Radio Frequency) protocols.

⁸ Rick Eyerdam, *Cargo Insecurity: Locals Offer a Better Mouse Trap*, **Florida Shipper**, May 28, 2007, pp. 7, 9, 76.

⁹ For a treatment of a series of DHS decision making, see Dr. James Giermanski, *DHS Decision-Making: Competence or Character*, **CSO Online.com**, January 2008.

¹⁰ James Giermanski, *RFID Is Not the One*, **Cargo Security International**, August/September, 2005, pp. 52-55.

¹¹ Jim Giermanski, *Trigger Point*, **Cargo Security International**, October/November, 2008, pp. 44-47.

¹² Giermanski, *DHS Decision-Making: Competence or Character*, 2008

¹³ **Smart Boxes**, A.T. Kearney, Copyright 2005.

¹⁴ Passive RFID devices respond only when activated by an outside signal emitted from a transceiver. A passive device has no independent power supply. An active RFID device has its own power and can emit a signal on its own without having to be triggered by a transceiver.

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 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 blast demonstration. 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 in writing 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. Yet, in the face of known risks, CBP is

continuing to use RFID as a standard at our ports, demonstrating its ignorance of this vulnerability or its lack of concern over it.

7. **In-bond or In-Transit Model**¹⁵

In-bond shipments to and within the United States are shipments not intended to enter the commerce of the United States and, thus, do not bear the requirement of payment of the appropriate import duties and taxes required under the law. To ensure the U.S. collects its duties in case an in-bond shipment does enter the commerce of the United States, U.S. Customs (Customs and Border Protection, or CBP) requires the posting of an import bond as security to guarantee payment. Bonded cargo is carried in sealed containers or trailers. Ordinarily, these conveyances with their cargo have a final destination outside the United States, but can transit through the United States to a border port of export or to a U.S. seaport for export. In-bonds also could have a temporary destination in the United States but not technically in the Customs territory of the United States, destinations like Foreign Trade Zones, or bonded warehouses.

The focus of CBP is on the identification of contents with respect to their value in the case of an “ad valorem” assessment of duty or their weight or size if it is a “specific” tariff. In effect, CBP is fundamentally concerned with tax collection, and thwarting the escape and evasion of taxes through smuggling operations. This was evidenced by CBP’s March 3, 2008 announcement of seizing more than \$67 million dollars worth of clothing illegally brought to the United States via the in-bond system. The shipment was supposed to transit through the U.S. Southwest to a Mexican destination. *“This is a significant example of yet another attempt to evade the U.S. textile trade laws,”* said Kevin Weeks, CBP director of field operations in Los Angeles.

Unfortunately for us, this CBP model or standard emphasizes revenue collection, not security. We have today, thousands of sealed containers from foreign shippers moving on our highways, at hundreds of foreign trade zones and bonded warehouses, and in motor carriers’ bonded distribution sites in the middle of cities and population concentrations like Yellow-Roadways distribution center in Charlotte, North Carolina. Regrettably, we don’t really know what these conveyances contain! We only know, as with the 24-hr. manifest, what they are said to contain. We also don’t know where they have been or what could have

¹⁵ For a fuller treatment, see Jim Giermanski, *Analysis: In-bond shipments, the Trojan Horse*, **Journal of Commerce Online**, March 19, 2008.

been placed in them at foreign transshipment ports or while in transit within the United States.

Following an investigation by the Government Accountability Office (GAO) that agency stated in its Report GAO GAO-07-561 of May 17, 2007: *The limited information available on in-bond cargo also impedes CBP efforts to manage security risks and ensure proper targeting of inspections. In-bond goods transit the United States with a security score based on manifest information and do not use more accurate and detailed entry type information to re-score until and unless the cargo enters U.S. commerce. As a result, some higher risk cargo may not be identified for inspection, and scarce inspection resources may be used for some lower risk cargo.*

There is no obvious excuse except the lack of knowledge or virtual incompetence of CBP's leadership that can be blamed for the present in-bond situation. The consequence is that CBP has not been able to improve our security by solving the in-bond problem. Both shallow knowledge and questionable leadership must be assumed. Even Mexico has recently implemented legislation to monitor arrival and departure, container location, length of stops, and access to the container or trailer while transiting Mexico.

8. Container Security Devices (CSDs) and the Science and Technology Directorate (S&T)¹⁶

My final example of DHS activity that is quite believable in light of what has been said so far is an example of an absolute waste and abuse of our taxes: the Science & Technology Directorate. One of the functions of the Science & Technology Directorate is to develop CSDs. S&T began this process in 2006. To date, it has not developed anything that can be used today as a container security device. However, the private sector, on its own, has! Because of what appeared to be DHS being out of touch with the reality of container security and the private sectors' advancement in this area, in September, 2009, DHS was requested to respond to 4 questions by a member of the U.S. House of Representatives. I think it's best to use the actual question and response from DHS to highlight the failure of S&T in developing a container security device.

1. *How much money has DHS spent since 2003 in creating CSDs, including the evaluation and development phases?*

¹⁶ Jim Giermanski, *Science & Technology Directorate of DHS: Do We Need It?*, *CSO Online*, September 21, 2009 http://www.csoonline.com/article/502663/Science_and_Technology_Directorate_of_DHS_Do_We_Need_It_?page=7

DHS S&T began developing Container Security Device (CSD) technology in 2006 in response to a requirement from CBP. The numbers reported below for CSD development, testing and evaluation are approximate as work (primarily T&E) for the CSD the Advanced Container Security Device technologies were funded via a single contract and conducted in tandem.

- a. FY06: \$3.9M***
- b. FY07: \$1.9M***
- c. FY08: \$1.9M***
- d. FY09: \$2.0M***
- e. Total Obligated to Date: \$9.7M***

2. *Have manufacturers received funding for the creation of CSDs?*

Yes. DHS S&T is funding two vendors to develop CSDs, Georgia Tech Research Institute and Science Applications International Corporation.

3. *Have the products used been found viable from these efforts?*

Yes, DHS S&T believes that at least one vendor will meet the performance requirements set forth by CBP. DHS S&T will deliver Open Performance Standards to CBP in Nov-Dec 2010 that will define the performance and operational characteristics for approved CSD technology.

4. *Have any of these products been deployed by the private sectors?*

Not yet.

I applaud them on their honesty. It is quite clear that they have, so far, failed even with a \$9.7 million dollar budget for this development. And assuming that they would have succeeded, we would likely have only a sophisticated (one hopes) door lock.

What is profoundly incredible is that DHS does not know that the world already has forms of CSDs that do more. Industry has already developed and is using containers that detect entry through any portion of it, report it automatically by satellite or satellite/cellular technology. Therefore, the containers talk and respond to a central control center and can send alerts of all types including radiation detection, etc. to whomever is set up to receive those messages. These containers also provide a literal chain-of-custody feature from stuffing at foreign origin with the identity of the person accountable for supervising and verifying the cargo sent to the authorized, identified, accountable person opening and verifying the cargo at destination.

And all of this not only exists but is being demonstrated in Europe and Asia and soon in South Africa, but particularly here on the Mexican border where it is being used today. Unfortunately, there is ignorance of the technological specifications of these technologies within DHS and CBP. Additionally, the engineering tests of the units actually operating in Europe have been found to be 100% effective and accurate.

Unlike the Department of Defense, homeland security has no industrial complex to develop its technology. It seems industry has done this for them free. Smart containers as they exist today, not only provide the security DHS can't seem to develop, but also make the supply chain visible and cheaper, making money for the user.¹⁷ It so happens to also provides security for the nations employing their use, including the United States. So what did we get for \$9.7 million dollars?

Conclusion and Final Grade

1. CBP's False Positive Standard: Grade - F

The 99% false positive standard is scientifically unsound given the environment of the global supply chain. Even medical science accepts less. For instance, if a man takes the prostate-specific antigen (PSA) test (which is not an absolute indicator of cancer), and if it indicated a need to look further, it would be reasonable to look inside to find out whether or not there is cancer. It just makes sense.

2. Legislation on 100% Scanning: Grade - F

Like the false positive standard, this model is unsound not only because of the worldwide and diverse treatment of containers in different ports and cultures, it does nothing to guarantee our security if a previously scanned container then goes through a transshipment port where a bomb, drugs, or gummy bears can be inserted prior to entry into the United States.

3. CBP's Container Management Standard: Grade - C- or D

With respect to container security, the U.S. lags, not leads. The gradual adoption of the *ISO 28000*, the research and development in and by the European Union, and the outbound and inbound, door-to-door standard established by the AEO program clearly demonstrate the lack of adequacy of programs such as C-TPAT and the level of

¹⁷ Dr. Jim Giermanski, *Cargo Security is Just Good Business*, *Logistics Today*, September 9, 2009, <http://penton.ebookhost.net/lt/ebook/7/index.php?page=4>

sophistication of CBP. Finally, this writer has demonstrated that an unknown shipper can send an outbound container through a major U.S. port without CBP knowledge of contents.

4. CSI and the 24-hr. Manifest: Grade - F

CSI's 24-hr. manifest not only doesn't tell us what is really in the container, it is filed by a 3rd party who takes the word of the shipper. While intended to improve security by having CBP personnel in foreign ports, it opens the door for other nations to have their Customs officials placed at our ports doing their thing! Finally, it is expensive to have our personnel there, especially in light of no linkage between them and what is actually leaving those ports in-route to the United States.

5. Sealed-Door Standard: Grade - F

Perhaps, the worst of all models is the seal-door standard. Suffice it to say that this writer has personally either accomplished or observed personally four ways of bypassing a sealed container without violating the integrity of the seal and without any manipulation of the hinges. In a public demonstration a sealed container was sent to private location where a philosophy professor and a housewife (trained for the purposes of the demonstration) surreptitiously breach a sealed container. It is shameful that DHS and CBP cannot or will not do better when systems that protect the entire container exist, and are affordable.

6. RFID Standard: Grade - F- (*if that's possible*)

As evidenced with the withdrawal of one of the major RFID manufacturers from the market, and the departure of another manufacturer from certain major ports, and as evidenced by scientific demonstration, RFID not only does not work for global container security, it remains a recognized vulnerability to our port system as confirmed by the Office of the Secretary of Defense.

7. In-bond/In-Transit Policy: Grade - F

Similar to the 24-hour manifest, we really do not know what is in the in-bond containers moving through and around the United States. We do know only what is claimed to be in the container. CBP and DHS know we know because just as the Office of the Secretary of Defense confirmed the vulnerability posed by RFID, GAO confirmed the security weakness posed by DHS' in-bond standard.

It's easy to give a grade, hard to teach, and even harder to learn. The U.S. has simply been lucky, complemented by a little stupidity on the part of the terrorists. Container security systems exist today to fix all of these weaknesses. And in response to J. Ahern,

there **is** proven technology to fix the transshipment problem. While other nations recognize this, CBP apparently does not. It's time for CBP to remove its head from where it is and learn.

8. CSDs and S&T: Grade - F

Perhaps the easiest, and most enjoyable (although I shouldn't enjoy it) "**F**" to give is the one to S&T. And they will spend \$9.7 million dollars to earn it. In response to the question as to whether any of their CSDs have been deployed by the private sectors, in their own words: *Not Yet!*