



http://www.csoonline.com/article/502663/Science_and_Technology_Directorate_of_DHS_Do_We_Need_It_?page=1

Science and Technology Directorate of DHS: Do We Need It?

James Giermanski says bungled container security initiatives call the S&T Directorate into question.

By James Giermanski

September 21, 2009 — [CSO](#) — There always seems to be something that DHS does that either doesn't make much sense, is a waste of funds, or is a little frightening. Perhaps the Department's recent Cargo Conveyance Security Technology Demonstrations of container security devices (CSDs) which took place at Sandia National Laboratory in Albuquerque, New Mexico is a little of all three. Unfortunately, it exemplifies the level of knowledge that DHS Science and Technology (S&T) Directorate has with respect to commercial applications of existing CSDs.

[Also see Container Security: Who's In Charge?](#)

It makes more sense to allow— instead of S&T—the operations components of DHS to determine the kind of research is needed to accomplish their mission objectives and be involved in its contracting. To demonstrate, an analysis of the recent presentation of CSDs by DHS in August, 2009 should support my thesis.

THE PLAYERS

1. Georgia Tech

From the coverage of the event, it appears that the Georgia Tech Research Institute (GTRI) with federal dollars developed and demonstrated two of the projects labeled "container security systems," although one might challenge the use of the word "systems," since one was merely detected the unauthorized opening or removal of the container doors. Without getting into the details of each, Georgia Tech, while a superb University with an equally superb research institute with great facilities and labs simply

has no depth in the area of container security. Specifically, technology for sensing that the doors have been opened or removed has been available for many years. Georgia Tech in 2006 announced that it was developing this capability.

A new shipping container security device in development by the Georgia Tech Research Institute could make U.S. ports less vulnerable to terrorist activities. The contract is funded by the U.S. Department of Homeland Security (DHS). Containers equipped with the new devices will be continuously monitored for unauthorized attempts to open the container doors, using a novel sensing technique that is sensitive to door angular position. The system will securely communicate container information remotely to port authorities, providing a log of door activity and an alarm if an event occurs that requires immediate attention.

The new device does not seem to do more than what already existed. In fact, we have had off-the-shelf sensors that are currently used to sense not just doors, but also entry into multiple sides of the container. Finally, GTRI's work in the container security area is mostly in RFID technologies which Georgia Tech admits is problematic given the lack of international standards for use in a global supply chain system.

2. SAIC (Science Applications International Corp)

According to Kenneth Concepcion, DHS/ Science and Technology, Border/Maritime Security Program Manager, SAIC is under contract to DHS S&T. The project title name is ACSID Six side solution system, as part of that contract we have second Task for SAIC, CSD just for the door solution, said Concepcion. The demonstration project took place August 17-28, 2009. Program Manager Concepcion further stated with respect to this demonstration: I should also point out that none of the vendors demonstrated anything at the demo, all demos were run by DHS S&T and Sandia National Labs who are under contract to DHS& It should be noted that this project began in 2006. Then in July 2009, the **Defense Industry Daily** announced: (SAIC) in San Diego, CA received a \$7 million indefinite-delivery/ indefinite-quantity, cost-plus-fixed-fee contract (N66001-09-D-0034) from the Space and Naval Warfare Systems Center (SPAWAR) Pacific to develop a container security device (CSD), a small, low-power sensor mounted on or within a shipping container to detect and warn of the opening or removal of container doors. The contract includes a 3-year ordering period without options.

So who is SAIC? According to the "About SAIC" section of its website, *We solve our customers' mission-critical problems with innovative applications of technology and expertise. In medical labs researching cancer cures, in the desert testing next-generation robotics, in the ocean deploying tsunami warning systems, SAIC people and technologies are there. In crime labs investigating new evidence, in Iraq helping protect and support our men and women in uniform, SAIC is there. It further states: SAIC has a strong commitment to supporting programs of national importance helping to solve or undertake our country's most significant problems. We offer a broad range of services and products to address our customers' most complex and critical technology-related needs. These services include the following: National Security, Environment, Critical*

Infrastructure, and Health. Counter Terrorism and CSD are included in its 116 areas in its Domain Expertise listing. Unfortunately, its National Security focus is clearly dominated by defense-related research. There is no listing of expertise in logistics or supply chain management. There also appears to be lack of industry perspective, specifically within domestic or international commercial operations.

Why then does DHS use research entities like GTRI and SAIC instead of looking to the logistics-connected industry for products which serve commercial operations, especially when commerce is the heart of container movement globally? There is no rational defense for avoiding practitioners linked to the supply chain industry or its service, especially in light of the undeniable and incontrovertible facts that industry already has developed and has available off-the-shelf CSDs that do more than what DHS is paying to develop. What is more disconcerting is that DHS' own Customs and Border Protection (CBP) component should know about all the advances in container security device development. Specifically, the World Customs Organization (WCO) has been involved in the research programs to develop and use CSDs.

WORLD CUSTOMS ORGANIZATION AND CSDs

The World Customs Organization (WCO) is the only intergovernmental organisation exclusively focused on Customs matters. With its worldwide membership, the WCO is now recognised as the voice of the global Customs community. It is particularly noted for its work in areas covering the development of global standards, the simplification and harmonisation of Customs procedures, trade supply chain security, the facilitation of international trade, the enhancement of Customs enforcement and compliance activities, anti-counterfeiting and piracy initiatives, public-private partnerships, integrity promotion, and sustainable global Customs capacity building programmes. The WCO also maintains the international Harmonized System goods nomenclature, and administers the technical aspects of the WTO Agreements on Customs Valuation and Rules of Origin.

Given the U.S. membership in the World Customs Organization, what relationship does DHS have with that organization with respect to supply chain security research and CSD development? On 17 June 2005, the WCO invited universities and research institutes around the world to meet at its headquarters in Brussels to discuss the possibilities of co-operation between the academic world and Customs in the field of capacity building. This was a first attempt at opening the Customs world to develop new technologies and techniques. One cannot find a U.S. university or research institute participating with the WCO. In 2006, the WCO called a conference to discuss partnerships in Research and Development (R&D). Again the U.S. was missing. In June 2008 WCO released the University of Le Havre study on the global impact of the US 100% maritime container scanning legislation critical of the U.S. decision. Then in 2008 at the trade symposium in Washington DC, Kunio Mikuriya, WCO Secretary General called for the tracking and tracing of cargo from origin to destination. The WCO will feature a treatment of smart containers in an up-coming issue of WCO Magazine. DHS has contributed nothing to the development and use of current CSDs that meet WCO requirement of origin to

destination control, tracking and tracing. In the face of this, DHS' Science and Technology Directorate is satisfied with concentrating on container door security, even though U.S. law now requires the tracking and tracing of hazardous cargo. In short, the DHS is simply out of the loop when it comes to CSDs.

One more piece of evidence of this is important to mention here. The European Union's Commission has created a program entitled the *Seventh Framework Programme (FP7)*. One aspect of the program, *SST.2007.2.1.3 Smart supply chain management in intermodal door-to-door container transport*, contains the following purpose statement:

The aim of the research is the reduction of logistics costs and maximisation of the efficiency, safety and security of the whole supply chain in global and European intermodal container shipment. The research will focus on the integration of information technologies, logistics and inspection including customs procedures. Activities will address research, development and demonstration of a full scale integration of:

- 1. technologies which enable the continuous monitoring and control of containers and the status of the cargo (the use of GNSS shall be considered),*
- 2. communication systems and platforms used by the transport business community and controlling authorities,*
- 3. supportive innovative procedures and processes in ports and terminals with the aim to establish seamless and high capacity container transport flows in the European and global supply chains.*

Expected outcomes will include: shared information system of vessel and cargo tracking accessible to shippers, operators and authorities; integration of multi-sensor information as to the conditions of the goods in containers, notably suspicious changes, into the shared information system; cargo handling processes and equipment interacting with the shared information system; alignment of information handling and customs procedures, contracting, and permitting. The above outcome should translate into verifiable benefits. International Cooperation is recommended for this topic in order to address transport of container at global level.

Not only does DHS not participate in FP7, its "doors only" and eventual "6-sided" breach detection mandate is an immature approach to container security and is quite obviously out of step when compared to the FP7 program. What's worse is that the FP7 program has already begun to evaluate existing CSDs and so far the CSDs' operational functionality has been 100% accurate. The piloting of CSDs that already capable of providing 6-sided and interior environment sensing is also taking place in Asia, Mexico, and soon in South Africa. Unfortunately DHS does not participate with the European Union, China, nor even Mexico in this regard. This non-participation is also disturbing in that the United States has signed an agreement with the EU to cooperate. The Agreement calls for among other matters, collaborative efforts in the container security area, identifying high risk containers, developing reciprocal systems for securing trade, and coordinating positions with respect to container security. At this time in the United States there are current CSDs already doing with DHS is trying to develop.

COMMERCIAL APPLICATION AND RESEARCH

Without DHS involvement, the commercial world has, on its own, developed CSDs that not only detect breaches, but detect breaches anywhere in the container. Examples of U.S. firms with existing container security systems are GlobalTrak, GateKeeper, FreightWatch, and SAVI. Current technology ranges from electronic door seals produced by Sealock and E.J. Brooks to "doors-only" RFID (Radio Frequency Identification), to satellite, to combinations of RFID, satellite, and cellular, to. The most sophisticated existing CSDs provide a chain-of-custody feature for the user, like GlobalTrak's CSDs. This type of CSD

- Electronically identifies the authorized personnel stuffing and securing the container, and accepts and report information like container/trailer number, booking data;
- Carries and reports logistics data, including container number;
- Detects and reports a breach in any part of the container in real-time or close to real-time;
- Tracks the container through the supply chain;
- Identifies authorized personnel unsealing container; and accommodates disparate logistics programs in communicating critical data.

The chain-of-custody CSD is also available in Europe through European DataComm (EDC). Both EDC and GlobalTrak can provide their services in many areas of the world at this time. Again, why is DHS trying to develop something that already exists and actually makes money for the user while also meeting WCO guidelines, AEO (Authorized Economic Operator) guidelines, C-TPAT (Customs Trade Partnership Against Terrorism) and other reciprocal security programs' guidelines around the world?

POSTSCRIPT

After professional, cordial, and productive communications between this author and DHS, I sent a communication to DHS stating the following:

In short, 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 accountable person who supervises and verifies 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, DHS and CBP do not know this. Additionally, the engineering tests of the units actually operating in Europe have been found to be 100% effective and accurate.

And industry has done this for its own reasons. Smart containers as they exist today make money. These containers make the supply chain visible and cheaper. It so happens to also provides security for the nations employing their use including the United States. Additionally, their use can provide a legal defense for the shipper or consignee because of the recent change in five rules of the Federal Rules of Civil Procedure which equate legally ESI (electronically stored information) to documentation.

If you would like specific information on their use, especially through our U.S./Mexican border, I can connect you to the supplier and user. I can also send you information in the way of Power Points or articles that explain more. When my WCO article comes out, I'll send you a copy.

DHS did respond by saying that container security technology will need to be recognized by the IMO (International Maritime Organization) which, of course, is false. Here's what DHS said:

In order for such technology to fully be applicable in all global supply chain operations and environments, the technology will need to be recognized and accepted as an instrument of trade by the IMO. Otherwise WCO around the world as well as various other regulatory bodies (Communications licensing and permits, Law Enforcement, Safety and Security) who would have statutory and regulation authority or responsibility on the operations and installation of such systems with regards to sea going container operations will not recognized such technologies internationally.

Here's what the IMO says:

The Maritime Safety Committee (MSC), its 82nd session from 29 November to 8 December 2006, and the Facilitation Committee, established a Joint MSC/FAL Working Group which met during the MSC session and began work on container and supply chain security, with a view to ensuring that the right balance is struck between enhanced security and the facilitation of maritime traffic. The Group, in its work, took into account the SAFE Framework of Standards to secure and facilitate global trade (the SAFE Framework of Standards) and the Authorized Economic Operator Guidelines, adopted by the World Customs Organization (WCO) in June 2005 and June 2006, respectively. The SAFE Framework of Standards was developed by WCO in response to a request from the 2002 SOLAS Conference which adopted SOLAS chapter XI-2 and the ISPS Code.

The facts are that there is no requirement or needed recognition by the IMO of container security systems for those systems to be used in global commerce. In fact, the IMO working group is a relative new entity with the IMO whose purpose is to facilitate WCO standards of container security practice like the AEO or C-TPAT, not in any manner recognize container security hardware. One of the fundamental issues in container security is that the world has no single international standard as exemplified by the

divergence of standards such as those of the ISO (International Organization for Standardization) with national standards like ANSI (American National Standards Institute), and industrial standards like EPC (EPCglobal, Inc. which alone is in about 100 countries). Additionally, no government is obligated to accept or implement any certain standard. This is especially true for container security.

DHS also said this: *Further the acceptance of any technology by either industry or governments will have to be open standards without any proprietary restrictions and to have a security valve from a DHS perspective that must be accurate and reliable in its detection and communications while in operations in any global supply chain route from time of stuffing to de-stuffing of the container and be without third party access to such* This response speaks for itself and appears to be its rationale for the role of S&T.

It looks like DHS is in an area about which it knows little, and is grasping for some validation. The fact remains: It is unlikely that it will learn much from universities and research firms with respect to the relationship between supply chain management and container security without input from or experience in commercial supply chain operations and in-the-field container security problems and challenges. DHS does not demonstrate depth or experience in the field that is necessary at decision-making levels to meet carry out its responsibility in facilitating end-to-end container security. Clearly, Homeland Security research can and should be done, but at what cost and result? Paying for R&D within DHS constraints like the requirement of a 99% confidence levels for CSDs in field usage, in uncontrolled handling and shipping environments, especially for use in container security, may be academically appropriate for laboratory work with pharmaceuticals, but pure nonsense for operational use in a global supply chain. More than that, spending tax dollars to develop what already exists, is not just wasteful, it's foolish, and naturally at the expense of more meaningful and productive research. DHS research should be driven by and in the direction of operational usage, efficacy, productivity, and commercial value since those who would use it must have a financial or efficiency return. ##

James Giermanski is President of Powers International, LLC.

Endnotes:

1. <http://www.gtri.gatech.edu/facilities>
2. <http://www.gtri.gatech.edu/labs>
3. <http://www.gtri.gatech.edu/files/GTRI-Annual-Report-2006.pdf>
4. <http://www.gtri.gatech.edu/news/inaugural-rfid-workshop-draws-irish-business-and-s>
5. e-mail message of September 9, 2009 at 12:12 p.m.
6. e-mail message of September 9, 2009 at 12:12 p.m.
7. <http://www.defenseindustrydaily.com/SPAWAR-Awards-SAIC-a-7M-Contract-to-Develop-Container-Security-Devices-05644/>
8. http://www.wcoomd.org/home_about_us.htm
9. <http://www.wcoomd.org/press/default.aspx?lid=1&id=7>
10. <http://www.wcoomd.org/press/default.aspx?lid=1&id=7>
11. <http://www.wcoomd.org/press/default.aspx?lid=1&id=160>

12. <http://www.wcoomd.org/speeches/default.aspx?lid=1&id=107>
13. Implementing Recommendations of the 9/11 Commission Act of 2007, Section 1554
14. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_304/l_30420040930en00340037.pdf
15. Robert W. Kelly, JD, Containing the Threat: Protecting the Global Supply Chain Through Enhanced Cargo Container Security, The Reform Institute, October 3, 2007, pp.8-9.
16. e-mail of September 10, 2009 at 11:27 a.m.
17. <http://www.imo.org/> under the "Container Security" link on its home page.
18. Jim Giermanski and Peter Lodge, Tolerating Reasonable Risk, Frontlines Column, Journal of Homeland Security, July 2007, p. 8, and Giermanski and Lodge, The Problem of Errors, DHS, and the False Positive' Standard, October 2007, http://www.homelandsecurity.org/newjournal/articles/giermanski_dhs_false_pos.htm
security information.