The Journal of Commerce Online

Analysis: A Fundamental Gap in C-TPAT

September 12, 2008 3:49:48 PM

James Giermanski / The JOURNAL of COMMERCE ONLINE

Customs and Border Protection helps to defend the United States by employing a layered security system composed of five layers. On April 2, 2008, before the House Committee on Appropriations, Subcommittee on Homeland Security, Deputy Commissioner of Customs and Border Protection, Jayson P. Ahern defined these five layers as:

-- The 24-hour manifest;
-- Screening through the Automated Targeting System (ATS) and National Targeting Center (NTC);
-- Customs Trade Partnership Against Terrorism (C-TPAT);
-- The Container Security Initiative (CSI) and Security Freight Initiative (SFI); and
-- The Non-Intrusive Inspection (NII) program.

While each has its unique function and purpose, clearly C-TPAT has been the most successful and probably the best of the five layers in effectiveness. However, C-TPAT has a significant and fundamental gap, a weakness easily exploited, yet disregarded by Customs.

Customs-Trade Partnership Against Terrorism

A general description of the program is best expressed by CBP itself. Begun in November 2001 with just seven major importers (emphasis added) as members, as of March 2008, the partnership has grown. Today, more than 8,200 certified partners that span the gamut of the trade community have been accepted into the program. These include U.S. importers (emphasis added), U.S./Canada highway carriers; U.S./Mexico highway carriers; rail and sea carriers; licensed U.S. Customs brokers; U.S. marine port authority/terminal operators, U.S. freight consolidators, ocean transportation intermediaries and non-operating common carriers; Mexican and Canadian manufacturers, and Mexican long-haul carriers. These 8,000-plus companies account for over 50 percent (by value) of what is imported (emphasis added) into the United States.

The Inbound Fixation

However, C-TPAT looks only in one direction. “C-TPAT recognizes that U.S. Customs and Border Protection can provide the highest level of cargo security only through close cooperation with the ultimate owners of the international supply chain such as importers

(emphasis added), carriers, consolidators, licensed customs brokers, and manufacturers." It clearly has an "inbound" focus, that is, it only seems to care about what is coming into the United States, although Custom's legal jurisdiction is both inbound and outbound. If one examines the program's security layers, it becomes quite clear that Customs is so concerned about containers coming in, that it ignores security related to containers leaving the Unites States. In other words, it is focused on a potential terrorist plan using a container loaded with a weapon of mass destruction shipped from a foreign location to the United States.

An examination of all the C-TPAT requirements for all the categories of participants confirms a 100-percent inbound fixation. Customs wants to know about the source of the incoming container, any business relationships between the foreign consignor and the U.S. importer-consignee, and almost everything one can think of in the way of information on the incoming container. By virtue of the 24-hour manifest, the cornerstone of another security layer, CSI, one can learns what Customs wants to know:

1. Carrier SCAC Code (Standard Carrier Alpha Code);
2. Last Foreign Port;
3. Vessel Name;
4. Voyage Number;
5. IMO Vessel ID Number;
6. Date of Departure from Port;
7. Container Number;
8. Commodity Description (with HTS-6);
9. Commodity Weight;
10. Bill of Lading Number;
11. Shipper Name and Address;
12. Consignee Name and Address;
13. Hazmat Code;
14. Seal Number;
15. Numbers and Quantity;
16. Foreign Port of Lading;
17. First Foreign Place of Receipt;
18. Vessel Country;
19. Date of Arrival at First U.S. Port;
20. Port of Unlading;
21. Time of Departure from Port.

These container and shipping data are not required of exporters' containers leaving the United States. Why not?

What is also disturbing is that in the European Union's Authorized Economic Operators' (AEO) program, the EU's counterpart to C-TPAT, outbound container movement is important. In the program's Definitions section, AEO makes the export security process equivalent to the import process. Authorized Economic Operators: defined in the SAFE Framework as, "…a party involved in the international movement of goods in whatever

function that has been approved by or on behalf of a national Customs administration as complying with WCO or equivalent supply chain security standards. Authorized Economic Operators include inter alia manufacturers, importers, exporters (emphasis added), brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors."

The AEO program also treats exporters in other than its Definitions section. For instance, Section B states: "The AEO shall maintain timely, accurate, complete and verifiable records relating to import and export (emphasis added). Maintenance of verifiable commercial records is an essential element in the security of the international trade supply chain." In the same section, the AEO requires the maintenance of "…records systems which permit Customs to conduct any required audit of cargo movements relating both to import and export (emphasis added)." Section D requires "Increased paperless processing of commercial shipments for both export and import."

While it is not the objective of this analysis to compare AEO and C-TPAT, it is reasonable to question why one program (AEO) clearly includes exporters and the other (C-TPAT) clearly excludes them.

The Export-risk Component

Somehow, U.S. exporters seem to have been overlooked as potential perpetrators of terrorism in Custom's layered approach to security. Customs has little, if any, knowledge of exporters, their legitimacy, business history, or financial soundness. Additionally, it is quite easy for a U.S. exporter to send a container destined for a foreign importer into a U.S. seaport or land port-of-entry. In fact, if this writer were to take out a port, he would do it from within, that is, obtain a container, load it with WMD (radiological waste, easily accessible in the U.S.) and explosives, seal it, create fictitious documents, use a legitimate, registered maritime or surface freight forwarder, or have it directly driven to the seaport or land port-of-entry by a motor carrier using fabricated documents.

Is there any basis in reality for this scenario? I think so. In 2005, a small, legitimate but unknown North Carolina international transportation security firm purchased a 20-foot container in one North Carolina city, took it to another city and had it modified (again for legitimate purposes) for a demonstration in another city of how easily it would be to enter a sealed container surreptitiously. After its use in the demo, the container was shipped to Europe. It was shipped in cooperation with a legitimate freight forwarder in yet another city who had no knowledge of the actual contents, if any.

Through the normal procedures of that freight forwarder, the sealed container was picked up and carried to a U.S. southern seaport where it was eventually carried to Europe. But there's more. Because of its use in the demo, it was further modified by the international transportation security firm to be easily accessible for clandestine entry for follow-on demos in Europe and to show how it could be used as a conveyance of WMD, drugs, or human cargo. In fact, that very container prior to its voyage to Europe was secretly entered, not by real terrorists but by a housewife and her accomplice, a philosophy

professor, placed a fake bomb and drugs into the sealed container as part of the U.S. demonstration. But, there's even more.

The IED (Improvised Explosive Device) Linkage

South African engineers of this same North Carolina firm believed that RFID usage, as approved for use with containers in the United States, could be a serious vulnerability because of the ease of detecting these RFID emissions. RFID emissions can serve as the trigger-mechanism for detonating an explosive device within the container. Because an explosive device can be easily wired to detonate with the proper RFID frequency signal at any of our nation's seaports and land ports, all our nation's ports that employ the approved RFID frequency for shipping containers become more vulnerable to terrorist attack.

Because the decision was made by the Federal Communications Commission to set aside a frequency of 433.5 to 434.5 MHz spectrum band, and allow these RFID systems to transmit for 60 seconds, rather than only one second, the North Carolina firm decided to test the IED trigger hypothesis. Therefore, in 2007 the same firm that demonstrated two years earlier that furtive entry into a sealed container was achievable, now showed how the use of U.S.-approved RFID frequency transmissions in our ports could be used as an IED (Improvised Explosive Device) to detonate that same type of container.

Representatives of the Office of the Secretary of Defense were present and confirmed the legitimacy of the demo. In the Department of Defense's own words, the "U.S. Army representatives examined the device and wiring and confirm that a commercial RFID interrogator was use to 'wake up' a commercial RFID tag. When the RFID tag responded on the 433 MHz frequency, the relay closed and the blasting cap set off the explosive charge."

The equipment needed to detonate the charge was available at Radio Shack and the detonator was prepared by an undergraduate engineering student at a North Carolina university. In preparing for the demo, the firm also discovered how easily it would be to detonate an outbound container in most, if not all, U.S. seaports and land ports-of-entry, particularly land ports-of-entry -- a chilling combination of factors!

In other words, that small North Carolina firm clearly proved the existence of two very important risks. First, that its subject container, while sealed, could be prepared to be accessed secretly, defeating the seal barrier, and that no Customs authority, in the U.S. or Europe, discovered its preparation nor its potential role as a potential WMD conveyance.

Second, it demonstrated how the use of the U.S.-approved RFID container security frequency could easily trigger explosives carried within a container. These two factors connected to an outbound export shipment of an unknown exporter demonstrate a clear gap and flaw within C-TPAT suggesting to Customs that it immediately modify C-TPAT to include equally, the export factor in port and homeland security.

Postscript

Representatives of Homeland Security declined to attend both demonstrations. Defense attended both demonstrations. Just one more indication of the level of leadership and concern for our security.

James Giermanski is chairman of Powers International Inc. and director of the Center for Global Commerce at Belmont Abbey College. He can be contacted at (704) 825-4741, or at powersintnlinc@bellsouth.net.

Footnotes

1. For a fuller explanation of these layers see Jim Giermanski, Container Security: Is the Layered Approach Working? CSO Online.com, June 25, 2008.

2. http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/port_security/ctpat_sheet.xml.

3. http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_overview.xml.

4. Jim Giermanski, Container Security: Is the Layered Approach Working?

5. Pamela M. Zaresk, Area Port Director, U.S. Customs and Border Protection, Charleston, S.C., Presentation at the Annual South Carolina International Trade Conference, May, 2007.

6. Authorized Economic Operators, World Customs Organization, Policy Commission, 55th Session, Brussels, June 9, 2006.

7. AEO, p. 7

8. AEO, p. 9

9. AEO, p.21