http://www.csoonline.com/article/411113/Container_Security_Is_the_Layered_Approach_Working_

Opinion

Container Security: Is the Layered Approach Working?

Guest columnist Jim Giermanski says the government's five-layered approach to container security is on the right track, but needs significant improvements

By James Giermanski

June 25, 2008 —

On April 2, Deputy Commissioner of Customs and Border Protection Jayson P. Ahern made a statement before the Committee on Appropriations, Subcommittee on Homeland Security, U.S. House of Representatives. One of the topics included in his statement was an explanation of the layers of security used by Customs and Border Protection (CBP) to protect the nation against potential terrorism connected to commerce through U.S. ports.

"CBP uses a multi-layered approach to ensure the integrity of the supply chain from the point of stuffing through arrival at a U.S. port of entry," he said, citing five layers:

- 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) the Security Freight Initiative (SFI); and
- The Non-Intrusive Inspection (NII) program.

The goal of this layered approach, he said, is to combine each of the layers while limiting their combined affect on "hindering the movement of commerce through our ports."

Some of those in the trade community might take issue with this statement, believing that the layered approach has already hindered commerce. Others might take issue with the value of the layered approach in preventing a terrorist attack on a port of entry or interior target within the United States. I think that looking at each layer is important in appreciating this approach to security. Understanding the basics of each layer will indicate the knowledge CBP will likely have of the actual contents of containers reaching the United States.

Layer-1: The 24-hour Manifest

In general, a cargo manifest is a document that indicates the identity and description of the cargo contained in a shipment. There is certainly no problem using data from the manifest to determine contents. However, the manifest is made by vessel carriers, shipping lines that have no idea of actual contents. Therefore, any problem will always be linked to the person or firm that completes the manifest and their real knowledge of the contents of a container. CSI's 24-hour rule places the responsibility of sending the manifest to CBP with the shipping line, specifically the liner that loads the cargo into the vessel at the foreign port, carrying it to the United States, and discharging the cargo in the United States. "Carriers and/or automated NVOCC's will be required 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:

- 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 loading 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 loading
- 17. First foreign place of receipt
- 18. Vessel country
- 19. Date of arrival at first U.S. port
- 20. Port of unloading
- 21. Time of departure from port

Furthermore, there's an expectation that CBP will announce in August or September the requirement to submit additional data contained in the "10-Plus-Two Program." There

will be 10 pieces of data the shipper will have to submit, and an additional two pieces that the vessel carrier has to submit. From reviewing only six customs forms connected to inbound shipments, there were 122 distinct pieces of information. Of these bits of information there were 26 pieces that were repeated in the six forms. If that is any indication, there are hundreds of pieces of information-data that are CBP's mainframes that may or may not really be necessary or accurate. Regardless of how many elements are in the manifest today, the fundamental reality is that all elements represent what the shipper, not an individual, said to be true. In effect, the manifest states what is "alleged" to be in the container.

But the purpose of the 24-hour rule is to enable U.S. Customs to analyze container content information before a container is loaded and thereby decide on its "load/do not load" status in advance. An NVOCC is a non-vessel operating common carrier. In reality that entity can be a motor carrier leasing space on liners. For instance, Yellow Roadway trucking company is an NVOCC. Therefore, it accepts cargo from a shipper and provides the shipper a bill of lading to destination, including ocean travel, but Yellow Roadway does not own or operate an ocean-going vessel. Yet, it still is the carrier to its shipper and then it's the shipper to the vessel carrier. But only those NVOCCs who are authorized to communicate with CBP through an approved electronic portal can file a manifest as the liner can.

There is a flaw in this layer. How does a carrier know what's in the container? The carrier does not open the container to inspect it. The carrier simply takes the word of the shipper. Who is the shipper? Does the carrier really know? Even if the carrier really knows, the carrier is still relying on the shipper's word for the contents of the container. What if we have a perfectly honorable and well recognized shipper? Does that mean that between the stuffing of the container at origin and its arrival at the port of export, no surreptitious entry was made into that container and no weapon of mass destruction placed in the container before it arrived at the port of export? Since the carrier does not know what is really in the container that arrived at the port, how would CBP know what was really in the container if CBP relied only on the carrier's manifest? Assuming the shipper has historically been honest and trustworthy, the likelihood of CBP suspecting foul play is remote or non-existent under this layered approach. Thus, any positive or special treatment given this container can be deadly to either the recipients of the container, the United States, or to the exporting port where the explosive could really have been meant to detonate.

Layer-2: Screening through the Automated Targeting System (ATS) and National Targeting Center (NTC)

CBP says that the ATS is one of the most advanced targeting systems in the world. "CBP uses ATS to improve the collection, use, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. Additionally, ATS is utilized by CBP to identify other violations of U.S. laws that are enforced by CBP." Basically, CBP through ATS collects various data from itself through CBP's own

systems, except for one, the Treasury Enforcement Communications System. These systems as they relate to cargo are the:

- Automated Commercial System (ACS)
- Automated Manifest System (AMS)
- Automated Export System (AES)
- Automated Commercial Environment (ACE)
- Treasury Enforcement Communication System (TECS).

The data obtained "includes electronically filed bills, entries, and entry summaries for cargo imports; shippers' export declarations and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers; land-border crossing and referral records for vehicles crossing the border; airline reservation data; nonimmigrant entry records; and records from secondary referrals, incident logs, suspect and violator indices, and seizures."

Although AMS and ACE are CBP-based, AES is not. "The Automated Export System (AES) is a joint venture between CBP, the Foreign Trade Division of the Bureau of the Census (Commerce), the Bureau of Industry and Security (Commerce), the Directorate of Defense Trade Controls (State), other Federal agencies, and the export trade community." It's a central point through which exporters and/or their agents identify the products they are selling abroad. It serves primarily for export compliance and export data used by the Bureau of Census. However, ATS does draw more data from one source that is not its own: TECS. TECS has access to the National Crime Information Data Base (NCIC) which allows further access to the National Law Enforcement Telecommunications System (NLETS). TECS also includes names of individuals on terrorist watch lists. The next obvious question is who analyzes the data. CBP uses the National Targeting Center.

The NTC was established in 2001 and provides target-specific information to CBP field offices. With more than 100 employees, the center works around the clock. According to CBP, "The NTC has given CBP the ability to identify previously unknown, as well as known, persons involved in terrorism." Analysts or targeters, as they are called by CBP, are CBP personnel. These targeters also do data mining to develop potential targets. CBP says that the targeting center looks at any resource that could support a terrorist effort, ranging from individuals to raw materials that could be used in constructing nuclear and chemical weaponry.

However, like most of the layered approach, the center does not have active "boots on the ground" collecting intelligence. Instead, it analyzes the same and similar data obtained from the 24-hr. manifest and from its numerous other Customs Forms. If the paper is wrong or incomplete, however, targeting can also be wrong or incomplete. In other words, while this NTC is very important, it still is a data center, relying on data, and not knowing what is really in any container coming to the United States.

Layer-3: Customs Trade Partnership Against Terrorism (C-TPAT)
In this layer, electronic data and paper data are also essential elements of CBP's security. However, the C-TPAT layer is different. C-TPAT, as announced in 2001, "is an import-oriented program that provides incentives to shippers, such as reduced cargo exams and first-in-line priority for inspections, in exchange for adopting tight internal shipment processes for themselves and overseas business partners to prevent terrorists or criminals from slipping contraband or weapons into a container. CBP checks that companies follow approved security plans that meet minimum guidelines by visiting a company's headquarters and conducting sample audits of some foreign suppliers and transport providers." It was and is a voluntary program for industry, initially focused on large U.S. importers and exporters, ports/terminal operators, and carriers. Other participants were added, and today it has 12 different categories of participants. It began with only seven major importers. In 2008 it has over 8,000 certified members. In the beginning, it had only seven security areas of concern with respect to the supply chain: business partner requirements, physical access security, personnel security, procedural security, personnel security, container security, and education/training security. Now it has more.

With C-TPAT, CBP accepts as true the data furnished by its participating entity unless it learns or knows otherwise. Like the ATS/NTC layer, and to some degree the CSI/SFI layer, information provided is only as good as the providers' knowledge or integrity. With C-TPAT, there are clear and mandated physical requirements for the C-TPAT participants, which, if followed, can and do contribute to the security of this nation. Additionally, in C-TPAT there are auditors who review actual participant procedures at real locations around the world. With C-TPAT there are "boots on the ground" actions, not only data acceptance.

Layer-4: Container Security Initiative (CSI); the Security Freight Initiative (SFI)
CSI addresses the threat to border security and global trade posed by the potential for terrorist's use of a maritime container to deliver a weapon. CSI proposes a security regime to ensure that all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. Its core elements are:

Identify high-risk containers. CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence.

Prescreen and evaluate containers before they are shipped. Containers are screened as early in the supply chain as possible, generally at the port of departure.

Use technology to prescreen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade.

Through CSI, CBP officers work with host customs administrations to establish security criteria for identifying high-risk containers. Those administrations use non-intrusive inspection (NII) and radiation detection technology to screen high-risk containers before

they are shipped to U.S. ports. CSI, as a reciprocal program, also offers its participant countries the opportunity to send their customs officers to major U.S. ports to target ocean-going, containerized cargo to be exported to their countries. Likewise, CBP shares information on a bilateral basis with its CSI partners. Japan and Canada currently station their customs personnel in some U.S. ports as part of the CSI program.

However, the CSI program is anchored in the 24-hour manifest rule. CBP officers are only allowed to physically inspect containers in the participating foreign country ports when authorized to do so by that nation's customs authorities. The CSI program is more dependent on data acquisition and analysis.

There is a link between CSI and SFI, but not an extensive one. First, SFI is a scanning project composed of radiation portal monitors to detect radiation through NII (non-intrusive inspection) imaging systems. NII is really intended for small package imaging and border crossing functions. The Secure Freight Initiative is active at only three ports at full capacity: Puerto Cortes, Honduras; Port Qasim, Pakistan; and Southampton, United Kingdom as opposed to the 58 foreign ports participating in CSI. It was active in a limited capacity at Busan, Korea; Singapore; Port of Salalah, Oman; and Hong Kong. However, because there are significant problems with the SFI project, further deployment of machines is being reviewed due to recent lessons learned as revealed by CBP Deputy Commissioner Jayson Ahern in his April 2 statement. Ahern specifically cited 13 problem areas with SFI.

Essentially, CSI like other layers is really anchored in data flow. Its validity is only as good as the accuracy of the data submitted. SFI is similar but slightly different. It's only as good as its operators and the sophistication of its technology. According to the trade community, it is inefficient and according to scientists, SFI is 100 percent ineffective for highly enriched, shielded uranium. The technology is still being developed. The project is limited in scope, and there is serious discussion about its acceptance and application around the world. In June, 2008 the WCO called for the repeal of a U.S. law requiring all inbound maritime cargo containers to be scanned at foreign ports by July 1, 2012. And on June 11 in a report to Congress, DHS released all of the lessons learned from the SFI operational ports. In light of what the report revealed, it is doubtful if the SFI will continue, given its level and sophistication of its development and technology and the objections of the other trading nations.

Layer-5: Non-Intrusive Inspection (NII)

NII is mobile gamma-ray imaging technology. It is deployed at seaports and at land ports of entry, permitting officers to detect and interdict contraband (such as narcotics, weapons and currency) hidden within conveyances and/or cargo while simultaneously facilitating the flow of legitimate trade and travel. The mobile gamma-ray imaging system employs a gamma ray source that permits officers to quickly see inside tankers, commercial trucks, cargo containers and other conveyances without having to physically open the conveyance and/or container. NII machines can scan vehicles up to 125 feet in length in one pass. One version of the system is mounted on a truck chassis and is

operated by a three-man crew. The NII operates by slowly driving past a parked vehicle with a boom extended over the target vehicle.

As a layer, NII is equivalent to "boots on the ground." It detects something it sees. It is not data-centered. While often the densities it reads may not turn out to be guns, drugs, or currency, but only something resembling them, it does have very clear security usage. In fact, NII has been used at the Super Bowl in 2008 and at NASCAR events in addition to its ports security duties.

Conclusion

While I have often criticized DHS and CBP for many of their decisions, policies, and management decisions, the layered system is fundamentally sound. It is sound in spite of the lack of active intelligence gathering and the lack of container security technological applications which are currently available. However, its weaknesses, while few, are significant. In fact, the tremendous reliance on submitted information on which to base security decisions is a weakness and needs to be addressed. While C-TPAT is good, a recent GAO (Government Accountability Office) report in May 2008, pointed out numerous areas of concern. There are also GAO reports on the effectiveness of scanning at border ports of entry.

It seems that the layered security concept needs two more layers. The first is an actual intelligence/counterintelligence layer. That will be a problem. A short, but true story will help to explain. In the late 1990s a young man came to my office when I was teaching at Texas A&M in Laredo. He knew that I was a colonel in the Air Force Office of Special Investigations (AFOSI), at that time a little known fact, and was told to contact me. He told me that he was an Air Force first lieutenant, and he said that he just finished the intelligence program at Fr. Huachuca and was just assigned to the Border Patrol.

When I asked why, he said that he was assigned there to teach them how to set up an intelligence net and that AFOSI sent him to me for guidance. Needless to say, even if he were successful, what level of intelligence gathering and counterintelligence capacity and ability would CBP have roughly 10 years later? Again, from personal experience with Customs (CBP) on cross-border drug movements, I found that CBP had little or no expertise in developing intelligence. Since it was not their job to do so, one can expect it would not be done. In fact, there has always been a stigma attached to CBP's law enforcement history and status. For many in law enforcement, and for some outside of law enforcement, CBP had the image of a government tax collector and border guard. However, as of July 6, 2008, CBP officers have law enforcement retirement coverage, indicating a significant change in the perception that many had of them. CBP now has federal law enforcement status. Under DHS, CBP clearly has enforcement status and all that should with it, including an intelligence function. While maybe not having it before given their historical role was understandable in the 1990s, it is not understandable today.

Also, today there should be greater cooperation between and among counterintelligence and law enforcement areas, unlike when I was an FBI agent. Yet, it seems that it may still

be a problem. What cooperation does CBP receive from those agencies that could help CBP in preventing terrorist acts? CBP's National Targeting Center should be fed more than CBP's own data. There should be, and hopefully there is, the sharing of intelligence collected by other federal law enforcement and intelligence agencies. Thus, the first new layer, the counterintelligence layer, could be attained, not by CBP's own operations, but through the cooperation of those agencies that currently conduct counterintelligence.

The second new layer, and probably the easiest to accomplish, is a layer of security provided by smart containers. A smart container system is more than just a locked door or an RFID (Radio Frequency Identification) tag. A smart container is one that can be questioned and can respond in real time or close to real time. It can tell CBP that it is being breached, moved, or used as a host for WMD. Specifically it has eight general characteristics.

- 1. It functions as a part of a system approach necessary to coordinate all facets of the supply-chain process to ensure visibility and security, beginning at origin.
- 2. It electronically identifies the authorized personnel stuffing and securing the container at origin.
- 3. It captures and transmits electronically certain trade data that will link to other supply-chain documentation, and accept and report information such as container/trailer number and booking data.
- 4. It complies with the WCO, C-TPAT and AEO (European Union's Authorized Economic Operator) requirements to maintain the integrity of the entire container, by detecting a breach anywhere into its body.
- 5. It reports in real time or as close to real time, any breach.
- 6. It provides worldwide geographic positioning throughout the supply chain when queried, and when programmed, automatically report its position if it is off its designated course of travel.
- 7. It recognizes and records the identity of the authorized person opening the container at destination.
- 8. It accommodates an array of sensors and is able to communicate with or be adaptable to varied software packages used by shippers and carriers within the supply chain.

The international call centers or control centers that interact with smart container messages also sever as third party verifiers of the container's integrity and global movement. Smart boxes are essential to improving supply-chain security. They must be included in CBP's layered approach. They already exist. Unfortunately, it appears that CBP does not know that.

All security systems are penetrable with enough time, money, knowledge or inside help. Good security systems limit that probability. The layered approach is good. It just needs to be better. And it can be better with two additions: "boots on the ground" counterintelligence and the use of smart containers.

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