Combining Commercial Benefits with Cargo Security Initiatives  
By: Captain Salloum, H.

Following the tragic events of September 11, 2001, the role of US Customs has been changed forever. Today, this agency has the extremely demanding, “dual challenge of protecting our citizens and our borders from terrorists and the implements of terror, while facilitating the flow of legitimate trade.” In response to this new challenge, Customs management has recently undergone extensive changes. Since April of 2002 eight of the top nineteen US Customs’ executives are new to their positions. To help improve cargo security, this team has taken the lead in designing new and innovative programs. These programs include C-TPAT, CSI, the “24-hour” rule, and FAST (the joint US/Canadian Customs program for the northern border). To date, most of these programs have been voluntary.

The international leadership of US Customs in developing plans to improve cargo and supply chain security is to be commended. The underlying concepts of exchanging information with appropriate international agencies to help identify suspect shipments, and including foreign ports and customs agencies in these plans are very important. Plans designed to identify high risk shipments and target them for further inspection enable the most efficient use of scarce customs’ resources, further improve the security of shipping networks, and help to speed-up the flow of legitimate commerce.

Still, overlaps exist in these plans. Shippers/receivers, carriers, and intermediaries are invited to join C-TPAT, FAST, and Project Shield America (covering exports). While CSI is designed for ports, the program impacts nearly every entity involved in shipping. Likewise, under the “24-hour” rule carriers must electronically file manifest information. Nevertheless, this rule affects all shipping participants. Since these overlaps involve only one government agency and these programs already lead to concerns amongst shipping participants, one may wonder about the following:

- What sort of overlaps will exist once the Office of Homeland Security becomes operational?
- What sort of overlaps will exist when international governments and the World Customs Organization introduce their own cargo security rules?
- Will these developments further cloud the picture as in the Canadian initiatives (CSA, CDRP, and PIP)?
- Why is there no coordinated, global approach to cargo security?

International port and cargo security needs to be approached from a holistic, global perspective. To be effective such an approach should consider the following guidelines.

- To be proactive, US Homeland Security agencies must collect real-time global shipping activity data and apply sophisticated artificial
INTELLIGENCE IN ORDER TO IDENTIFY AND FLAG SUSPICIOUS SHIPMENTS, REGARDLESS OF PORT OR COUNTRY OF ORIGIN.

- When addressing US national security, it is crucial to cross check data from official sources with private sector data to test for integrity and consistency.
- US national security should not depend on the integrity or capability of a single source of information or individual data sources in foreign countries.
- Limitations in technology capabilities in foreign countries should not hinder the flow of timely quality data from any foreign country.
- Despite any political or cultural differences, US agencies should be able to receive reliable data from foreign countries.

Keeping these rules in mind, let us now consider three primary US Customs programs; the Customs Trade Partnership Against Terrorism, the “24-hour” rule, and the Container Security Initiative.

C-TPAT is the Customs Trade Partnership Against Terrorism. This private/public sector partnership involves US Customs inviting private companies involved in the flow of a shipment, from shipper to receiver, to help improve international supply chain security by applying “best practices” for security to their organizations.

C-TPAT is a good concept and the underlying ideas of voluntary “best practices” programs to improve supply chain security sound reasonable. Yet, officials within homeland security have stated that mandates will be required in order to truly improve cargo security on the large scale. Proposed cargo security legislation and the new Office of Homeland Security provide previews of mandates to come.

On the global scale, corporate shipments are vulnerable based upon the realities of international shipping. C-TPAT members may have the most secure organizations, contract only secure suppliers, and utilize secure intermediaries and still have their shipments delayed or hijacked based upon the following reasons:

- C-TPAT cargo mixes with less secure cargo on the same vessel.
  (The significance of this is amplified by rulings that if a suspicious container is flagged while on board a ship, that ship will be denied entry into US ports until the suspicious container is discharged onto a barge, six miles off shore).
- Corporate shipments may be used by terrorist as a cover-up for their activities.
Carriersnet asserts that in order to effectively deal with these issues, a holistic, global approach must be implemented. A comprehensive security system should be enabled that addresses corporate and individual shipper’s shipments as well. In order to encourage the maximum involvement of private companies, this overall project must be built on the basis commercial benefit.

The top twenty-eight ocean container carriers represent approximately eighty percent of the global movement of sea containers. Therefore by establishing twenty-eight secure data connections, the majority of global shipping data will be accessed. Applying artificial intelligent to this commercial data and establishing two monitor lists, Enterprise Monitor List (EML) and Shipment Monitor List (SML) will enable new capabilities to flag suspicious enterprises involved with a given shipment and/or a suspicious shipment itself.

Shipments will be monitored for data mismatches, data anomalies and shipment flow deviations. In other words, through integration with corporate shipper supply chain management systems, the SML will identify the responsible parties who load, survey and move shipments throughout global supply chains. In addition, the system will know how long various events should take and how long they actually took (forecast vs. actual). This capability will be enabled by the process of combining global events with satellite tracking.

This approach has been independently validated by other organizations that recognize the strengths of enhancing official programs with private sector initiatives. In its recent Cargo Security

White Paper the National Customs Brokers and Forwarders Assoc. of America, Inc. (NCBFAA) outlined some ideas to enhance C-TPAT and cargo security. In particular, they summarized a “Chain of Custody Dataset” or CCD. The CCD looks very much like the EML and SML approach. According to the NCBFAA, the CCD “… will provide the deep penetration into supply chain risk evaluation that is necessary to detect security risks from the remotest source to the final receiver.”

The “24-hour” rule states that ocean carriers must electronically submit completed shipment manifest information to US Customs, via their Automated Manifest System, 24-hours prior to loading vessels bound for US ports. As of December 2, 2002, US Customs made this rule mandatory. This rule has also become law under the Port and Maritime Security Act of 2001 (S.1214).

By far the most controversial plan that has been proposed to address cargo security is the “24-hour” rule. There has been considerable resistance from the private sector to the “24-hour” rule. For example, in extensive comments to US Customs concerning this matter, World Shipping Council President Christopher Koch articulated several industry
concerns with this plan. Mr. Koch and the forty-plus ocean carriers he represents are greatly concerned about the negative impact the “24-hour” rule may have on their businesses.

There are also several security and operational problems associated with the present over-emphasis on the shipment manifest in existing cargo security plans. The shipment manifest was never intended to be an informational resource to enhance cargo security. The shipment manifest is the sum of bill of lading associated with a vessel/voyage. It is noteworthy that the shipment manifest is a key component of S.1214 which, “requires ships to electronically send their cargo manifests to a port before gaining clearance to enter, and prohibits the unloading of improperly documented cargo.”

The ultimate sources of manifest information are the shippers. In essence, the system is relying upon shippers to be honest about what they are shipping. And when certain officials were asked how they would confirm that manifests are filled out correctly, they proposed to ask the freight-forwarder. This begs the following questions:

- How will the freight forwarder actually know what was in a container?
- How effective is any process for identifying suspect shipments that relies on shipment manifest information provided by shippers?

The freight-forwarders only charge nominal fees to submit bill of lading instructions on behalf of shippers and they could be in different cities, freight forwarders do not actually know what is in a container. Therefore, the only person who actually knows what is in a container is the shipper. In essence, there are two principal issues associated with relying on shippers to provide information used to screen their own shipments.

- How can government agencies be certain of any given shipper’s integrity?
- Even when a shipper is reliable, can his shipment still be hijacked by terrorists?

Once again, enabling EML and SML capabilities will help to confirm or deny the integrity of shippers and/or shipments on the global scale. Intelligently analyzing historical private sector shipping data concerning large and small participants involved in a shipment and introducing real-time monitoring of shipment data will help address the issues outlined above. In addition, incorporating the systems of land, air, and/or ocean carriers will provide up-to-date information about the actual movements of the international freight of corporate and individual shippers.

CSI is the US Customs Container Security Initiative. The idea behind CSI is “pushing back the borders” to the port of origin. This plan involves stationing US Customs inspectors in foreign ports to assist the pre-screening of containers bound for the US. Initially, the top twenty
mega-ports, representing “roughly 68 percent of the 5.7 million sea containers entering the U.S. annually” have been invited to join CSI. To date, fourteen of these foreign ports have signed on.

Due to the nature of the shipping business, ships that are employed on regular service typically call about eight ports per voyage on average. Therefore, their itineraries are not limited to mega-ports. The common links between these ports is the vessel. Therefore, a given port could invest large amounts of resources to address the security of cargo moving through their port, and yet a ship sailing from this secure port could be denied entry into a US port due to suspicious containers that were loaded at smaller ports that are not part of CSI.

Additional political and economic factors have emerged that bring the present design of CSI into question. For some time, US ports have been concerned that the “24-hour” rule may provide a competitive advantage for Canadian ports. This is due to the fact that shipments being unloaded in Canadian ports, ultimately bound for the US via road or rail, are not subject to the “24-hour” rule. US ports have legitimate concerns that cargo may be diverted from US to Canadian ports as a result.

A new perspective on CSI came to light in a NY Times News Service article “Port Security Plan Irks Europeans” (11/6/02). According to this report, “European Union officials are concerned that the program’s incentives favor those ports that sign the agreements and penalize those that either refuse or are too small to take part.” Likely, cargo that has been pre-screened at CSI ports will be subject to less rigorous inspection at US ports than non-CSI shipments. EU officials state “that companies shipping goods to the United States will start rerouting their cargo to ports like Rotterdam, depriving others of business and potentially creating bottlenecks in some shipping regions.” As if to drive home this point, ‘A Dutch customs official (stated) the US agreement was not just a way to prevent terrorist attacks. “It’s good for business,” she said.’ The EU views European Customs agreements as European Community agreements. Therefore, “the EU is considering the possibility of beginning infringement procedures against countries that have signed on to the initiative.”

Since the common denominator regarding international ocean freight movements are ships, not ports, methods to confirm the integrity of containers aboard ships must be put into action. Incorporating vessel specific information into the EML and SML system will improve the intelligent screening of cargo at any port and terminal. When integrated into port security and customs operations, this approach will improve the targeting of cargo for scanning or inspection by customs officials. This technique will help address the competitive and operational issues associated with the present design of CSI. Significantly, this approach has been recognized by top officials within US Homeland Security Departments as “ahead of the game.”

Commercial Benefits
As a commercially viable e-logistics solution designed to standardize and
Simplify shipping processes and deliver positive ROI for shipping participants, the Carriersnet system offers the global shipping industry sophisticated smart business tools that enhance the reliability and dependability of logistics networks by bringing shippers and carriers closer together, helping organize the private shipping market, and improving logistics providers’ service delivery. Since these private enterprises are profit motivated, the costs associated with enhancing cargo security should be offset by a system that provides economic benefits as well. Following are key benefits such a system should deliver for select members of the global shipping community.

**Carriers:**
- Unique tools for managing capacity utilization and minimizing dead space.
- Organizing the private shipping market.
- Minimizing non-value added activities between shippers and carriers, increasing carrier and shipper ROI.
- Enhancing relationships with contracted corporate shippers via integration into global supply chain management systems.
- Compliance with new and emerging international governmental cargo security regulations.

**Corporate Shippers:**
- Integrating Just In Time Inventory with JIT Shipping.
- Global Coverage and Tracking.
- Global Visibility (status, freight costs, survey).
- Global Documentation and Claim Processing.
- Automated Exception Processing.
- End to End Real Time Performance Monitoring.
- Compliance with new and emerging international governmental cargo security regulations.

**Individual and Small Shippers:**
- Allowing shippers to evaluate and select carriers serving desired destinations, based upon individual shipment needs.
- Allowing shippers to obtain real-time rate quotes, complete bookings, submit bills of lading, and more online, in a few minutes.
- Providing shippers with access to information concerning customs, insurance, financing, and warehousing, etc.
- Allowing, for example, an Italian shipper moving cargo from Brazil to South Africa, with door-to-door shipment to obtain personalized service provided through the selected carrier’s local agent networks.
- Standardizing and expediting claims processes.
- Standardizing and expediting documentation processes.
- Delivering global coverage using multiple carriers and multiple modes of transport.
- Enabling real-time global tracking by combing GPS with event status reports.
Ports:
- Cost effective means to target suspect shipments for inspection prior to loading.
- Cost effective means to target suspect shipments entering the home country.
- Providing smart tools to help plan and maximize port capacity utilization.

Delivering commercial benefits for all participants in global logistics is the basis of Carriersnets’ worldwide PCT patents, priority date June 1999. In analyzing the needs of homeland security, company management quickly realized the system’s unique features and functionality can improve cargo security by intelligently collecting and organizing global shipping data to enable new enterprise and shipment monitoring and screening capabilities, as outlined in this article. This approach places Carriersnet in the distinctive position of helping to enhance cargo security, while improving the efficiency of private companies’ global logistics networks.