GLOBAL COALITION
FOR EFFICIENT LOGISTICS

CAPT. H. SALLOUM
PRESIDENT & CEO
AXIOLOG

to

U.S.House of Representatives Select Committee on Homeland Security

On

"BEST BUSINESS PRACTICES FOR SECURING AMERICA'S BORDERS"

WASHINGTON, D.C.
JULY 23, 2003

Confidential

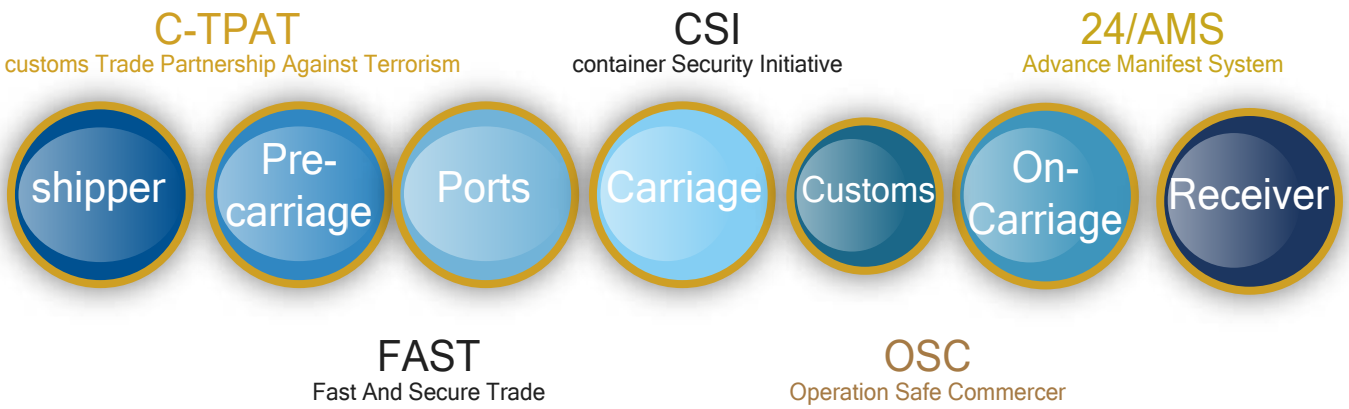
INTRODUCTION

The leadership of the U.S. Department of Homeland Security in developing plans to protect our borders is to be commended. This department through the Customs & Border Protection 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.”

Following September 11, 2001 multiple Homeland Security programs have been launched to protect our borders from terrorist incursions via commercial shipments. These programs include Operation Safe Commerce (OSC), The Container Security Initiative (CSI), Customs Trade Partnership Against Terrorism (C-TPAT), and the Advance Manifest System (AMS).

These initiatives have been created to address specific subsets of shipments. In essence, the flow of a shipment has been broken down by tasks. This is due to the fragmented nature of international shipping. To illustrate, a relatively simple lane from a GM Silao assembly plant in Mexico to dealerships in Jacksonville, Florida involves 19 shipping events with 11 different companies, each employing their own proprietary information management systems. In global lanes, transshipments and consolidations can significantly increase the number of events and participating organizations.

For years, the global shipping industry has been seeking new methods to integrate these participants in order to improve efficiency and boost profits. Yet, no end-to-end system to manage this industry exists today. Given this reality, the U.S. Department of Homeland Security had little choice but to concentrate enforcement efforts on specific entities. This has led to overlaps. For instance, one shipment may be impacted by five different initiatives from the Customs & Border Protection alone. Any given entity may also be impacted by multiple initiatives.



As shown above, shippers/receivers, carriers, and intermediaries are invited to join C-TPAT and FAST. While CSI is designed for ports program may impact nearly every entity involved in shipping. Likewise, under the “24-hour” rule carriers electronically file manifest information. Nevertheless, this rule affects all shipping participants, since this information is supplied by shippers and may delay delivery if it is not presented properly. Since these overlaps involve only one government agency and these programs already lead to concerns amongst shipping participants, they may wonder about the following:

- What sort of overlaps will exist once the Office of Homeland Security becomes fully operational?
- What sort of overlaps will exist when international governments and the World Customs Organization introduce their own cargo security rules?
- Why is there no coordinated, global approach to cargo security?

Combining Efficiency and Security

The global economy demands efficient and secure global logistics. For any security system to be embraced worldwide, it must include commercial benefits. In other words, efficiency and security must go hand in hand. Efficiency by itself may compromise security. In contrast, overarching cargo security rules and regulations could damage the economy. Therefore, a comprehensive public/private sector solution must be implemented in order to economically and effectively deal with cargo security challenges. To encourage maximum private-sector involvement, the overall solution must deliver commercial benefits.

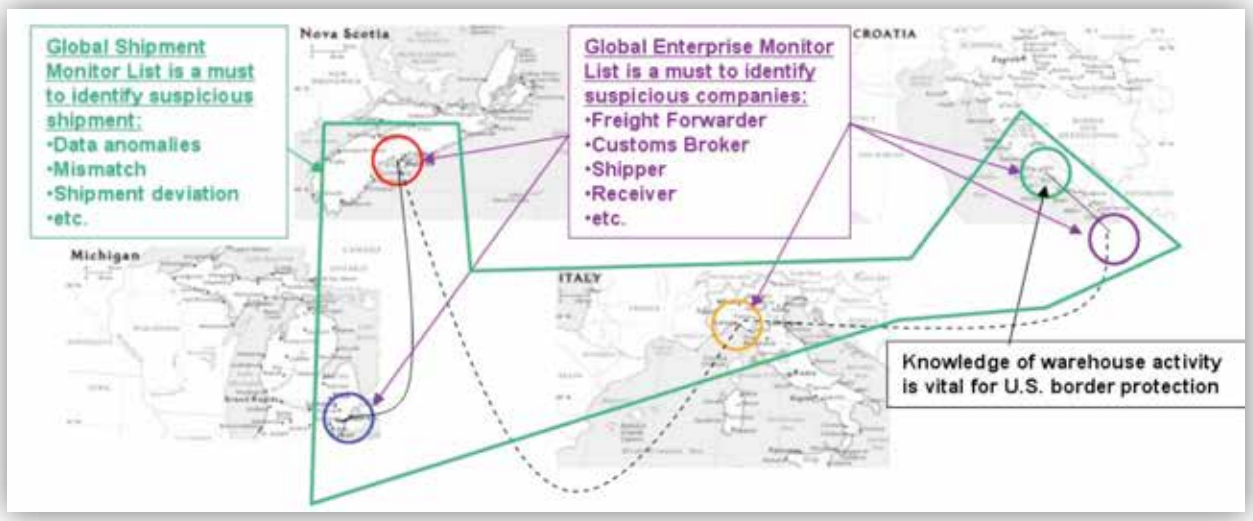
As an illustration, consider sea ports.Ports around the world are now being squeezed by seemingly opposing forces.

- Requirements of security initiatives to provide for more inspections, and improve the security of facilities.
- Pressures from shippers and carriers to process cargo faster and more efficiently.
- Real business needs to contain costs and improve profitability.

Failing to accommodate all of these forces will lead to imbalances that may result in financial losses, delays in the processing of cargo, and/or compromised security. None of these developments is acceptable.

We assert that to effectively address cargo security whether domestically or internationally, a holistic system must be enabled that takes the entire flow of global shipments into account, from the empty container in a depot to the final receiver.
Such acomprehensive approach must strive to meet two core objectives; 1) Encourage widespread private sector involvement by improving the process efficiency and profitability of all parties involved in shipment flows, and
2)Deliver cargo security improvements from the private sector that complement and reinforce official rules and regulations.

Cargo Security Guidelines Require Global Visibility



Suggested cargo security guidelines include:

- To be proactive, U.S. 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 U.S. national security, it is crucial to cross-check data from official sources with private sector data to test for integrity and consistency.
- U.S. 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, U.S. agencies should be able to receive reliable data from foreign countries.

Further, to effectively help protect the United States, modern technology should provide proactive information to multiple security agencies. To illustrate, consider the example of containers entering the United States by ship.

Intelligence Agencies: The system must provide historical shipping data to intelligence agencies about the warehouse where the containers were

loaded. Coast Guard: Proactive information should be made available to the United States Coast Guard about the contents of the ship and what is in the containers. The Coast Guard will then know specific details about the ship and its cargo, at any point in its voyage. This will enable the Coast Guard to stop and inspect suspicious vessels while they are still in international waters. Customs: At ports and border crossing, Customs agents should be provided with additional smart tools to flag suspicious shipments or enterprises. However, to effectively improve door-to-door security, information flows can not end at the border crossing. FBI,State Police, and local law enforcement: Once the cargo moves from the port of entry for in-country delivery, the system can continue to automatically track the shipment. If at any time the shipment deviates from its route a signal may be sent automatically to responsible officers. This scenario provides end-to-end cargo security.

Cargo Security Initiatives Enhancement

Keeping the above guidelines and scenario in mind, let us now consider how the following three primary Customs & Border Protection initiatives can be enhanced; the Customs Trade Partnership Against Terrorism, the “24-hour” rule, and the Container Security Initiative.

Customs Trade Partnership Against Terrorism

C-TPAT is the Customs Trade Partnership Against Terrorism. This private/public sector partnership involves 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.

Issues

C-T PAT is a good concept and the underlying ideas of voluntary “best practices” programs to improve supply chain security are reasonable. Yet, officials within homeland security have stated that mandates will be required in order to truly improve cargo security on the large scale. New cargo security legislation and advanced manifest laws provides 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.
- Corporate shipments may be used by terrorists as a cover-up for their activities.

To address these issues, a comprehensive security system should be enabled that addresses high-volume and low-volume shipper's shipments as well.

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 accessible. Applying artificial intelligence 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 Advance Manifest System

The "24-hour" rule states that ocean carriers must electronically submit completed shipment manifest information to Customs & Border Protection, via their Automated Manifest System, 24-hours prior to loading vessels bound for U.S. ports. As of December 2, 2002, Customs & Border Protection made this rule mandatory. This rule has also become law under the Port and Maritime Security Act of 2001 (S.1214). Effective October 21, 2003 this law will be expanded to include truck, rail, and air. Reporting times vary by mode. For instance, the interim ruling states that truck carriers must submit their electronic manifest information from 30 minutes to 1 hour before they arrive at U.S. border crossings.

By far the most controversial law designed 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 Customs & Border Protection 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 have expressed concerns about potential negative impacts the “24-hour” rule may have on their businesses.

Issues

There are also several security and operational problems associated with the over-emphasis on shipment manifest information in existing cargo security plans. The shipment manifest was never intended to be an informational resource for cargo security. The shipment manifest is the sum of bill of ladings 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 self-reported by shippers?

Since freight-forwarders only charge nominal fees to submit bill of lading instructions on behalf of shippers, they can not afford to physically inspect shipments. Therefore, freight forwarders do not actually know what is in a container. 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 or her 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

The Container Security Initiative

CSI is the Customs & Border Protection Container Security Initiative. The idea behind CSI is "pushing back the borders" to the port of origin. This plan involves stationing Customs & Border Protection 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" were invited to join CSI.

Issues

Due to the nature of the shipping business, ships that are employed on regular service typically call on 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. A given port could invest large amounts of resources to address the security of cargo moving through that port, and yet a ship sailing from this secure port could be denied entry into a U.S. 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, U.S. 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 U.S. via road or rail, are not subject to the "24-hour" rule. U.S. ports have legitimate concerns that cargo may be diverted from U.S. to Canadian ports as a result.

Another perspective on CSI came to light in a NY Times News Service article "Port Security Plan Irks Europeans" (1102/6/). 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 U.S. 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 U.S. 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." Even though a compromise was reached to avoid this suit, it points out how cargo security rules may have unintended consequences.

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 U.S. Homeland Security Departments as “ahead of the game.”

Commercial Benefits

Any commercially viable e-logistics network should be designed to standardize and simplify shipping processes for shipping participants. It should offer smart business tools to enhance the reliability and dependability of logistics by bringing shippers and carriers closer together, helping organize the private shipping market, and improving logistics providers’ service delivery. Increased costs of enhancing cargo security should be offset by a system that provides economic benefits. Following are key benefits such a system should deliver for 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.

High-Volume 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.

Low-Volume 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,and submit bills of lading online.

- Providing shippers with access to information concerning customs, insurance, financing, and warehousing, etc.
- Providing, 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 combining GPS and/or RFID 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 must be the basis of any security system. This approach will place that system in a distinctive position of helping to enhance cargo security, while improving the efficiency of private companies' global logistics networks.

Conclusion

In order to tackle the significant potential threats posed by the massive volumes of domestic and international cargo shipments, any solution must be commercially viable and be able to rapidly scale to handle high transaction volumes. Such a global solution must also provide methods to include every entity involved in the global shipping industry (land, air, and sea) into a cohesive cargo security strategy. To encourage maximum private-sector involvement, the overall solution must provide clear commercial benefits.

Axiolog appreciates being invited to address this committee, and looks forward to assisting your continued efforts in protecting America's borders.