



[www.apllogistics.com](http://www.apllogistics.com)



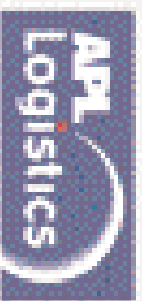
[www.apl.com](http://www.apl.com)

**Neptune Orient Lines**

456 Alexandra Road  
NOL Building  
Singapore 119962  
[www.nol.com.sg](http://www.nol.com.sg)

# Stronger Links:

**Adding Security and Value to the Supply Chain**



# Table of Contents

<b>Executive Summary</b> .....	<b>1</b>
<b>1: A Transportation System Built for Speed</b> .....	<b>4</b>
Ship First, Ask Questions Later	
Pressure Points	
<b>2: Thinking Inside the Box</b> .....	<b>6</b>
International Initiatives	
Washington's Response	
Key Programs in Place	
<b>3: Industry Approaches</b> .....	<b>8</b>
Operation Safe Commerce	
Technological Initiatives	
<b>4: A Supply Chain Security Checklist</b> .....	<b>10</b>
<b>5: Conclusion</b> .....	<b>13</b>
<b>Sources</b> .....	<b>14</b>
<b>About AP/L/APL Logistics</b> .....	<b>15</b>
<b>At a Glance</b> .....	<b>16</b>

# Executive Summary



In the wake of the September 11, 2001 terrorist attacks in the United States, there were two aspects that stood out in particular as the focus turned to seeking to prevent such horror ever happening again: the terrorists' planning took advantage of the relative openness of U.S. society, and their implementation involved 'off the shelf' commercial transport as both the weapon and the delivery system.

This has huge implications for the complex transportation system that supports the massive volumes

of goods flowing throughout the world as part of global trade – and for those who use and operate that system.

Some 7.8 million loaded containers enter U.S. seaports annually – an average of more than 21,000 daily. Another 4.8 million containers pass through the same terminals and gates carrying export cargo. A significant number of containers move through ocean and inland networks empty, being repositioned to pick up new freight bookings.

An end-to-end supply-chain move can involve as

many as 25 parties and 35 to 40 shipping documents. On a single inbound sailing to the U.S., a typical modern container ship sailing 80 per cent full might today be carrying 3,000 containers of various sizes and thus generate, transmit and manage more than 100,000 documents.

This white paper is offered from the perspective of two hands-on participants in global supply-chain management. APL and APL Logistics operate across more than 87 countries providing services that include

freight-management, end-to-end electronic monitoring, consolidation or deconsolidation, Singapore-flag, U.S.-flag and foreign-flag container-shipping, and intermodal connections.

The security picture continues to change daily, and not even an overall framework yet exists in which the different initiatives fit. This paper cannot begin to answer all the questions that lie ahead. Instead, its purpose is to raise supply-chain-wide issues with the aim of contributing to an effective and balanced response.

Key conclusions include:

***1. Close co-operation between and within the public and private sectors is vital to tightening security without compromising supply-chain efficiency and the flow of global trade.***

Co-operation is highlighted in two U.S. Customs Service programs – the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) – that provide a regulatory blueprint for future global supply chain security efforts.

CSI “pushes back the border” for U.S. import cargo, requiring electronic filing of detailed cargo manifests, including key data points, to be provided 24 hours in advance of loading the cargo at foreign origin ports onboard ships bound for the U.S.. Because of the length of time it can take to sail to the U.S., this will impact in terms of weeks and fundamentally change long-established documentation practices. This carries associated cost implications for manufacturers, shippers and carriers.

*It is impossible to physically inspect each container in transit, even using modern scanning equipment, without*

*bringing global trade to a grinding halt.*

C-TPAT is a voluntary security program aimed at establishing uniform standards for secure facilities, assets and equipment, procedures and personnel for various parties throughout the supply chain. Membership of the program and compliance will mean avoiding unnecessary delays in cargo clearance by minimizing U.S. customs inspections and audits.

***2. As these initiatives are expanded, manufacturers and shippers at the head end of the supply chain will bear increasing responsibility for ensuring container security, and for providing complete, accurate and timely documentation when loading.***

More so than in the past, they will need to know their customers, suppliers and vendors; to secure and restrict access within cargo facilities; to supervise and verify container loading and affixing of tamper-proof seals; generate, verify and transmit manifest information earlier; and provide information to allow screening of cargo against a risk profile as far back in the supply chain as possible.

***3. Supply chains will become increasingly centralized. This does not mean having to reinvent the wheel.***

Because of the numerous points of vulnerability of a global supply chain, placing all or most of the operations into the hands of a single, centralized management agency – whether internal or outsourced – provides better protection against unauthorized tampering with merchandise or data.

While today’s third-party logistics (3PL) networks were originally designed to expedite the flow of goods and information and to provide security against such threats as pilferage and insertion of illegal substances into shipments, many of the processes and safeguards they employ are applicable, with varying degrees of modification, to deterring terrorism.

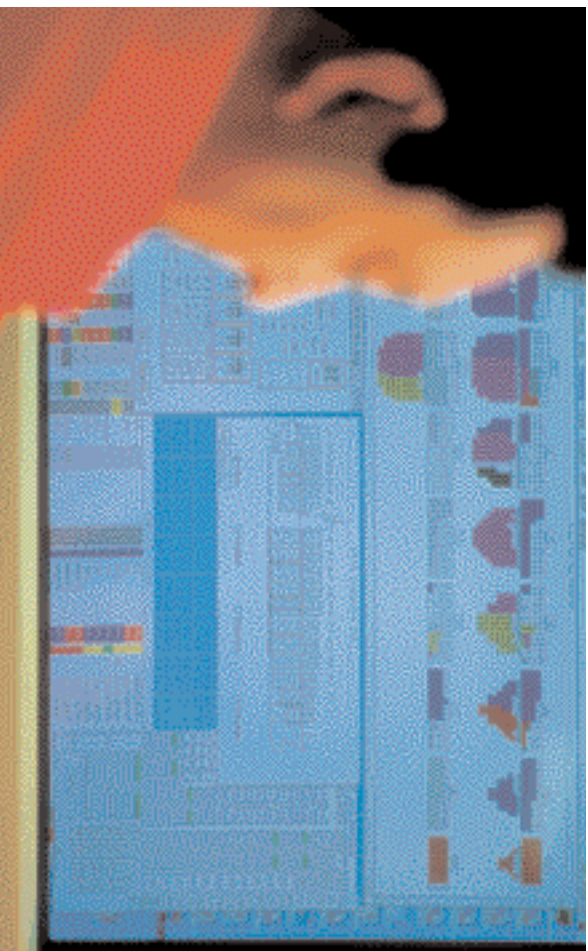
***4. The costs of the additional steps to further safeguard supply-chain security could be in the billions, with some estimates as high as US\$10 billion. These costs need to be spread equitably among those benefiting from heightened security – including, in many cases, the broad public.***

Washington, D.C.-based Brookings Institute estimates their proposed anti-terrorist recommendations related to U.S. coastal protection, seaport security, and cargo security would total US\$5.3 billion. Additionally, Brookings points to another US\$10 billion or more that Customs could spend for additional, comprehensive programs related to road, rail, air and sea that would raise the costs, but produce less risk of failure.

Not included in the Brookings estimates were foreign port security enhancements, private IT investment, or costs associated with developing and implementing new security programs at private manufacturing and assembly facilities in the U.S. and abroad, or at the facilities of foreign and domestic vendors to these manufacturers.

***5. Technology already plays a critical role in supply-chain security and its importance will skyrocket. But investment in technology, itself, without systemic changes in business practices at every level, will not be the hoped-for panacea.***

Automated entry of documentation should ideally be pushed back as far in the supply chain as possible, preferably to the beginning. However, the issue remains that not all manufacturers and shippers, or indeed, countries, have the infrastructure and the IT tools, personnel and training to be able to input data, supervise the load and count process, audit documentation and identify and report discrepancies.



# 1: A Transportation System Built for Speed

*Container transport promises fast transit time, smooth handoffs and continuous flow of goods and inputs; security raises the question of what's actually moving.*

At its inception in 1956, containerization of ocean freight was intended to streamline commerce.

The first container ship, a converted tanker, carried truck trailers bolted to the deck from New York harbor to Houston. The idea was to speed loading and unloading, minimize cargo handling and related costs, reduce pilferage and damage, and make shipment tracing easier.

Nearly 50 years later, a complex global network of ships, dedicated trains and trucks, specially-designed terminals and gates and transloading/consolidation warehouses – supported by information technology and the Internet – has made the promise of supply-chain integration a reality. This potent transportation-technology combination has enabled manufacturing businesses to view and manage in real time the flow of raw materials, components, assemblies and finished product across a global enterprise, from factory to retail store shelf or end-user.

Businesses ranging from auto makers to supermarket chains to fashion apparel houses to chemical and pharmaceutical companies increasingly manufacture and ship on a just-in-time and, in some cases, even a build-to-order basis. Production inventory once measured in weeks or months is now often measured in hours or, at most, days. Thus manufacturers are able to slash inventory carrying costs and respond instantly to changing customer demands.

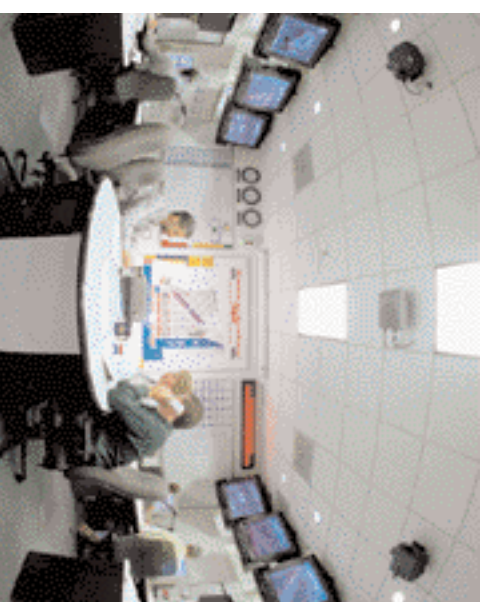
Cass/ProLogis, in its annual State of Logistics report, estimates total 2001 annual U.S. business logistics costs – including inventory, transportation, warehousing,

technology and administrative – at US\$970 billion, or 9.5 per cent of GDP, down from 10.1 per cent in 2000 and from 16 per cent of GDP in 1980. During the period from 1980-2000, inventory carrying costs fell 37 per cent, and transportation costs were cut by 22 per cent, largely due to transportation deregulation, integration of materials management and physical distribution systems, increased efficiencies and advances in information technology.

These dramatic gains in productivity and reductions in cost rely primarily on a system of trust, under which inventory moves unimpeded through the supply chain in sealed containers that are loaded, transported, stored, staged, handed off among parties and delivered to their ultimate destinations intact and on schedule. A set of shipping instructions, usually based on the shipper's purchase order and container packing list, either accompanies the shipment when it is received at its origin port or follows a short time after. Shipping instructions provide the customer, cargo, country of origin, routing and end-user information that generates final bill of lading and cargo manifest documents.

## Ship First, Ask Questions Later

Logistics providers have little choice but to assume that bill of lading and cargo manifest information is complete and accurate, given the volume of freight in the global pipeline and complexity of the system. Each year more than 800 scheduled vessels of all kinds make 22,000 calls at 361 U.S. river and seaports. Approximately 7.8 million container loads of cargo entered U.S. port



gateways in 2001 – an average of more than 21,000 truckloads daily.\* Another 4.8 million containers carried export cargo from inland and coastal origin points to those ports, and nearly 2.5 million 48-foot and 53-foot containers were deployed in purely domestic service.

At any given time, millions of empty domestic and international containers also move through the system, being repositioned for pick-up of specific loads or to trade lanes where demand is high. *Containerisation International* reports more than 236 million 20-foot equivalent unit (TEU) container moves in 2001 and more than 203 million TEU moves in 2000, based on port and terminal figures collected worldwide.

A single international container move can involve up to 25 parties, from the factory or warehouse to

\*Based on conversion of cargo statistics showing 11.3 million inbound and 6.7 million outbound twenty-foot equivalent units (TEU) moving through U.S. ports, using industry multiplier of 0.7 to reflect actual number and proportion of 20-, 40- and 45-foot containers used. A commonly quoted figure of 5.7 million inbound containers is less precise – it divides the TEU number in half since most container cargo moves in 40-foot units.

the origin port, to and from the ship, at each handoff among transportation providers and at each step of the warehousing and distribution process. It may involve trading companies, banks issuing letters of credit and various transportation intermediaries. It may involve consolidated loads on behalf of multiple shippers, in a single container. A complex end-to-end move can generate 30 to 40 shipping documents. Thus, a modern 5,000 TEU containership sailing 80 per cent full might carry shipments generating an average 98,000 inbound documents alone in one sailing. And container ships are getting larger, with several of 7,000 TEU carrying capacity or more in service, and even larger ships being planned.

Stopping a container in transit, processing the necessary paperwork and inspecting it by hand takes five customs officers three hours. An inspection station using state-of-the-art mobile scanners requires fewer people and can process up to 11 containers an hour. Not surprisingly, fewer than 2 per cent of arriving containers – and a smaller percentage of export loads – are subjected to full inspections, usually where documentation questions arise or the shipment meets a high-risk profile based on the shipper, consignee, cargo, country of origin or routing. Random inspections of empty containers and use of mobile scanners and radiation detection pagers has increased overall screening in recent months.

Since the September 11, 2001 attacks, however, a global container transportation network designed for speed and flexibility must be viewed through the added lens of different security considerations. Given the estimated US\$737 billion value of total container trade moving through U.S. seaports annually, it is a matter of



serious commercial interest for any business that manufactures, buys, sells, ships, insures or manages a supply chain globally.

#### **Pressure Points**

The supply chain has numerous points of security vulnerability. In this era of global sourcing and manufacturing, a manufacturing or retailing importer may have little detailed knowledge of the day-to-day operations of contract factories and suppliers halfway around the world. Logistics providers frequently deal with new or unknown shippers and consignees, based on little more than a credit report.

Container transport is a common carriage system. Shippers and consignees are not necessarily known

entities, and they may not even know their own suppliers, subcontractors and customers well.

Containers bound for the U.S. are routinely handed off among a number of inland transportation intermediaries – freight forwarders, truck drivers, barge operators – on their way to the port of origin, and then transferred between small regional feeder ships and large linehaul container vessels at transshipment ports. In some parts of the world, they may wait for days in terminals that may or may not be fully secured by fences, lighting, surveillance and gates, and whose employees may or may not have been subjected to background checks. In many locations, freight arrives on ships uncontainerized and is then moved to containers, and while container seals are ideally tamper-proof, standards vary widely.

Containers have been used in the past to smuggle narcotics, conventional weapons, quarantined plant and animal species, cigarettes and alcohol, counterfeit merchandise and illegal aliens. Since September 11, the list of criminal uses has expanded.

Of greatest concern to the U.S. Government is the prospect of a nuclear, biological or chemical weapon being smuggled in a container and detonated either in port or upon arrival in a major destination city. Without increased security measures of some kind, the basic unit of the supply chain – the ocean and intermodal container – has the potential to become the next basic unit of terror. Beyond a certain point, however, security measures in themselves have the potential to achieve a simpler, far more likely terrorist goal – disruption of global trade and transportation based on the threat of an attack alone.

## 2: Thinking Inside the Box

*U.S. Government sets new rules and standards for container security.*

Already indicated, the sheer volume of container traffic worldwide precludes comprehensive container inspections, which, anyway, to be effective would need to be done at the place where the cargo was loaded into the container. That means instead that the advance information collected about the contents, routing, status and the people handling that container must be accurate, up to the minute and available immediately, with an enforced goal of zero tolerance.

This detailed information must be collected, beginning at loading and throughout the end-to-end move. An exception process must be in place to identify, isolate and examine suspect shipments quickly, minimizing the impact to the flow of normal supply-chain operations. And at each step in the supply chain, facilities will have to be secured with respect to perimeters, procedures and personnel.

Some of these measures require international cooperation, others are the logical function of national governments, and many are best handled by the private sector, requiring close cooperation of manufacturers, shippers, suppliers and their transportation and logistics partners. Efforts to date break down as follows:

### **International Initiatives**

The United Nations' International Maritime Organization (IMO) is coordinating with the World Customs Organization (WCO), International Labor Organization (ILO) and the Organization of Economic Cooperation and Development (OECD) to address security issues surrounding vessels at sea and in port,

including wide deployment of vessel identifier and positioning equipment, installation of alarm systems, secured perimeters and security jurisdiction for ships in port, greater transparency as to ownership and control of vessels and standardized seafarer screening and identification.

An IMO working group has also proposed shipping trials involving 40 containers a week in three major global trades, using existing ocean carrier cargo information and shipment tracking capabilities to develop a standardized international container security program by late 2003.

### **Washington's Response**

The U.S. administration is currently undertaking a massive government reorganization that will centralize the functions of some 100 agencies – among them the Customs, Immigration, Border Patrol, Coast Guard and Emergency Management functions – under a single Department of Homeland Security in order to facilitate cooperation and information sharing.

The Maritime Transportation Security Act 2002 mandates and initially funds port vulnerability assessments and security planning; harbor terminal personnel screening and training; expanded Coast Guard vessel escort and boarding programs; increased U.S. Customs Service staffing and purchase of container screening and detection equipment; international security standards and programs involving cooperating foreign seaports; and vessel pre-arrival notification, including full advance crew, passenger and cargo manifests. It will also fund pilot programs to test security strategies and new technologies.



### **Key Programs in Place**

Two federal security initiatives already up and running promise to have the most wide-ranging effects on supply-chain planning: U.S. Customs' Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT).

CSI represents an effort to "push back the borders" by pre-screening, identifying, segregating and inspecting high-risk U.S. import shipments before they are loaded aboard ships at foreign origin ports. It initially focuses on the 20 largest ports that currently serve as origin and transshipment points for 68 per cent of all container shipments to the U.S., and could later be expanded to the next ten largest ports and beyond.

Risk criteria include a nexus of factors such as the shipper's identity and business, country of origin,

CSJ represents an effort to “push back the borders” by pre-screening shipments before they are loaded aboard ships at foreign origin ports; C-TPAT participants meeting security compliance standards are eligible for faster cargo processing at port gateways and border crossings.

commodity description and routing. Questionable shipments will be diverted and pre-screened at the port or an off-dock location. New U.S. Customs regulations require shippers and their supply-chain partners to provide detailed cargo manifest information at least 24 hours before containers are due to be loaded at a foreign origin port destined for the U.S.. Since September 11, 2001, the U.S. Coast Guard has required this information 96 hours in advance of vessel arrival at its first U.S. port. This new requirement will impact in terms of weeks, however, because of the length of time it can take between loading at a foreign port and arrival in the U.S..

Some 14 data points are required, including complete shipper and consignee information; a precise description or Harmonized Tariff Schedule classification for the cargo (which does not currently exist at any level); number and quantities from the master bill of lading; carrier, vessel, voyage, container and seal numbers; country of origin, first port of loading and arrival date in U.S. port; and hazardous material indicators.

C-TPAT has its roots in earlier Customs Service programs aimed at stopping narcotics and other contraband, in particular the Business Anti-Smuggling Coalition (BASC). Companies enroll in the program and sign a memorandum of understanding that commits them to perform a self-assessment of their current supply-chain security, and develop and implement a security program based on C-TPAT guidelines. Security compliance focuses on facilities, access, procedures, personnel, documentation and training.

Participants meeting security compliance standards are eligible for faster cargo processing at ports of entry; dedicated commercial lanes; an assigned Customs Service point of contact; account-based payment of duties; and reduced inspections and compliance audits.

At first limited to large charter member importers such as General Motors Corp., Target Corp. and Motorola, the program was expanded in July 2002 to include sea, air and rail carriers, as well as ports. In August transportation intermediaries – customs brokers, freight forwarders and non-vessel operating common carriers – were added. C-TPAT eligibility will be extended over time to port authorities, terminal operators, warehouse operators and manufacturers.



# 3: Industry Approaches

*Business explores pilot programs and new technologies to balance security and supply-chain agility.*

SI and C-TPAT together provide a blueprint for the regulatory environment in which manufacturers, shippers and logistics partners are likely to be operating in the future. But in the short-term, the trade community has voiced concern over the flood of overlapping regulatory, program and funding proposals, and their possible unintended consequences.

CSI, for example, will require bilateral cooperation and other countries may insist on the reciprocal right to push back their borders and inspect cargo at the U.S. end. Importers and intermediaries lobbied to submit advance manifest information directly to Customs rather than to carriers, and resisted the requirement of cargo descriptions at a six-digit Harmonized Tariff Schedule level of detail, for practical and competitive reasons.

Industry generally supports the U.S. Government's broad security mandate, but in that context is pressing for:

- **Clear, uniform guidelines establishing procedures and responsibilities**
- **Regulations that do not compromise the free flow of trade**
- **Government agency cooperation and sharing of data**
- **Use of data from existing commercial sources whenever possible**
- **International cooperation to secure the entire supply chain**
- **A means of recovering costs.**

As the push for heightened security moves forward, small and mid-sized businesses are concerned they could ultimately face a grim choice under C-TPAT: they can spend disproportionately to remain in compliance or be placed at a competitive disadvantage in the entry and treatment of their goods at U.S. ports. Importers also complain of shouldering the cost burden for tighter security that will benefit the broader public.

In a study prepared in May, 2002, the Washington, D.C.-based Brookings Institute, a public-policy think tank, issued a series of anti-terrorist recommendations related to U.S. coastal protection, seaport security, and cargo security. The costs that would be incurred for Brookings' "preferred options" totaled US\$5.3 billion, including budget increases for U.S. Customs and the Coast Guard, and improved port security, planning and personnel (at U.S. ports). Additionally, Brookings pointed to another US\$10 billion or more that Customs could spend for additional, comprehensive programs related to road, rail, air and sea that would raise the costs, but produce less risk of failure.

Not included in the Brookings estimates were foreign port security enhancements, private IT investment, or – drilling deeper into the supply chain – the costs associated with developing and implementing new security programs at private manufacturing and assembly facilities in the U.S. and abroad, or at the facilities of foreign and domestic vendors to these manufacturers.

While it is hard to quantify exactly, there is no doubt the additional costs needed to increase security along the entire U.S.-inbound supply chain will be counted in the billions of dollars.

One possible supply-chain security scenario for the future involves a tiered system of self-imposed security levels. Businesses would adopt a level of security that was necessary, achievable and affordable in accordance with their needs. The higher the level of security maintained and verified throughout the chain, the less a business would be subjected to delays due to inspections, examinations and audits. Such a system, however, is still a long way off.

Until such time as cost, competitive and operational issues can be satisfactorily addressed, the likely U.S. response in the event of a terrorist attack is still immediate

closure of U.S. ports, as was the case after the September 11 attacks. Such a response, for any prolonged time period, would pose as serious and immediate a threat to U.S. economic security as an attack would pose to physical security. Industrial disruption in 2002 on the U.S. West Coast gave a flavor of the sort of impact that could have.

## **Operation Safe Commerce**

Industry has sought to work through the tangle of recent government security proposals with a set of "real-world" pilot projects testing actual movements of freight across global supply chains.

Operation Safe Commerce (OSC) is a program developed by ports, shippers and transportation/logistics providers to test the security of shipments through major U.S. load center ports – Los Angeles/Long Beach, New York/New Jersey and Seattle/Tacoma – and to evaluate various security strategies and improvements to address weaknesses.

In one OSC pilot project reported in the *Journal of Commerce*, Ostram-Sylvania Corp. tracked an inter-company containerload of automobile tail lights from a factory in Eastern Europe to its Hillsborough, N.H. distribution center and evaluated security at each step. A Port of Los Angeles/Long Beach project, in which APL is a participant, will conduct threat and vulnerability analyses for sample shipments transhipped via Singapore to Los Angeles – and, in a second phase, to Chicago and New York. It will then assess new security procedures, facility upgrades, IT solutions and employee and cargo screening technologies.

Congress has authorized US\$28 million for various OSC pilot projects in fiscal year 2002-03. The Department of Transportation has awarded more than US\$92 million in grants for harbor security assessments, upgrades and pilot technology programs.



The ports of Seattle, Hong Kong and Singapore have begun a separate pilot project to monitor 2,000 containers moving from Asia through the Pacific Northwest port gateways with electronic security seals developed by Savi Technologies and using Qualcomm mobile communications technology. E-seals have also been tested on containers moving from Japan through Seattle and on to Canada as part of the Department of Transportation's Intelligent Transportation Systems (ITS) program. However, these do not provide enhanced security above the current manual high security 'barrier' type bolt seals, which also carry unique identification – and the issue remains that seals and other such initiatives do not provide information on what is inside the container.

### **Technological Innovations**

Technology will play a critical role in future security efforts. A number of technological advancements are already in the development and testing phases, or commercially available.

Two areas where government is likely to play a role – through public-private partnerships and under contract to research facilities such as Lawrence Livermore Laboratories in California or Sandia National Laboratories in New Mexico – will be: to develop technical standards in response to real-world threat and vulnerability assessment data; and to provide incubator funding for mass commercial production of new technologies where needed, to bring down per unit costs and ensure quick deployment.

Among the emerging products considered key to future supply chain security are:

**Radio Frequency Identification (RFID) tags,** fastened on the outside of a container, carry information on the container's contents and location in the supply chain. The data is transmitted over wireless frequencies as it passes electronic readers at various load, discharge and transfer points.

**Optical character recognition** electronically scans and records containers and chassis by unique identification code upon entering, leaving or moving within a terminal or warehouse, eliminating the need for manual entry.

**Global Positioning Satellite (GPS) and Global Locator System (GLS)** tracking uses satellite signals and transponders to determine the precise, real-time global location of containerships, rail cars, trucks and containers.

**Electronic seals** are applied at the time a container is loaded, often attached to the physical container seal and sometimes linked to sensors inside the unit. They maintain an electronic record of the container in transit, including time and location if a container is opened or tampered with. 'Smart' seals can also store shipment data

and transmit alerts that include GPS location coordinates at the time of opening or tampering.

**Radiation/chemical detection sensors** that can be placed inside the container – or on container-handling equipment at a terminal – would alert supply-chain parties and authorities to the presence of certain chemical fumes or higher-than-normal levels of radiation that would prompt closer examination of shipping documents and possible inspection.

**Vehicle and Cargo Inspection System (VACIS) mobile scanners** use gamma rays to see through container walls and perform non-invasive inspections. A scanning arm passes overhead along the length of the container in five to six minutes and the scan appears on a computer monitor.

**Radiation 'pagers'** are handheld devices approximately the size of a Palm Pilot that are being issued to customs inspectors nationwide. When passed along the length of a container they detect abnormal radioactivity.

**Biometric identification systems** involve fingerprint and/or retinal scans stored digitally on identification cards. Scanners compare the holder's fingerprint or retinal scan to that of the card and either permit or deny entry to secured areas based on job classification and clearance information also stored on the card.

**Container profiling software** now in development will access and cross-reference commercial and government data on shippers, origin-destination pairs, commodity descriptions and other data. In so doing, it will identify shipments with suspicious characteristics and create automated exception alerts for those containers.

# 4: A Supply Chain Security Checklist

*The keys to increasing security and value are the same: better information and tighter procedures.*

It is likely that CSI and C-TPAT compliance standards will drive the establishment of a new set of global security standards, possibly through the 159 customs administration members of the World Customs Organization. These, plus the results of pilot risk assessment and security improvement projects, can be expected to force important changes in the management of global supply chains.

Three trends in particular seem to be emerging:

- **Migration of security and documentation responsibilities toward the manufacturer/importer at the beginning of the chain**
- **Centralization of supply-chain processes under a single party with the ability to manage multiple supply-chain assets and vendors via an integrated IT platform**
- **Outsourcing of supply-chain integration and management functions to a third-party lead logistics provider (LLP), particularly those with assets and operational control, to take advantage of specialized expertise, partner relationships and economies of scale.**

Whether managed in-house or through an LLP, an ability to see the big picture of the supply chain, effect technical and operational changes across the entire chain, understand the technicalities of security compliance, and control costs, will be critical as companies pursue the dual-track goal of security and value.

Where supply-chain productivity concerns itself with streamlining for speed and flexibility – stripping out unnecessary steps, decision-making layers and so forth – security considerations focus on thoroughness. It is less about slowing down processes than about ensuring that processes are done correctly as planned, and that no gaps exist which permit unauthorized activities to take place. Security concerns focus on four key points in the supply-chain move:

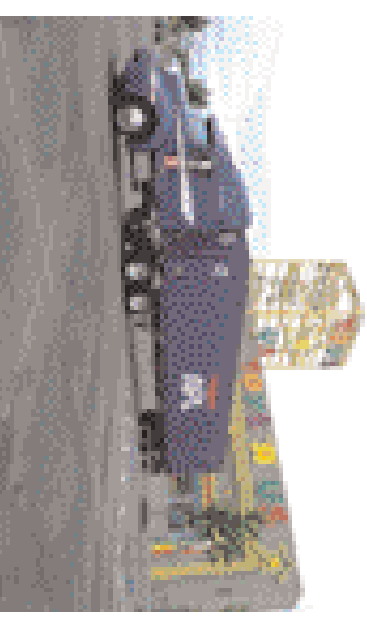
## *Container loading*

At present, a freight booking generates release of a container to the customer's premises and trucking arrangements, for pick-up of the cargo. The container may be sealed by the manufacturer or shipper at time of loading, or by the ocean carrier at time of receipt at the origin port container yard. Mechanical container seals vary in their resistance to tampering, from indicative seals – wire or plastic strips bearing their unique container identification numbers – to barrier seals that are heavy bolts bearing the identifiers.

These procedures are expected to change to barrier seals due to security concerns. In all cases, the shipper will likely be responsible for providing and affixing tamper-proof seals at time of loading in accordance with C-TPAT or comparable international standards.

## *Documentation*

Ocean bill of lading and cargo manifest data typically derive from Shipping Instruction and container



yard receipt information – in other words, initiating documentation prepared after the container is loaded and at the time it is received for loading aboard ship. This overrides information taken by the carrier at the time of booking, which may often be different as transaction terms and shipping decisions change.

From a security standpoint it is preferable to capture and enter this initial bill of lading information as early as possible in the supply-chain process – at minimum as the container is loaded and sealed, as verified against the purchase order. When linked to the specific container and verification of the container seal, this data forms the basis of all subsequent shipping documentation a step further back in the chain. Electronic replication of it throughout the move eliminates errors through re-keying that might prompt exception alerts and subsequent delays.

Single-party responsibility and asset control are particularly advantageous in maintaining the security of goods in transit.

Beyond what is in the container, information on the shipper-of-record, consignee, country-of-origin, destination and routing are also important. Matching these and other data points with container loading information is central to cargo pre-screening efforts under programs such as CSI.

All of these steps place new burdens on shippers and logistics providers to hire and train factory employees, truck drivers and terminal employees in data entry; introduce stricter procedures for weighing, counting and certifying cargo and equipment; report shortages and overages; and spot and report inconsistencies. It may also entail placing audit personnel on factory premises, or installing enterprise resource planning software and systems.

Several shipping companies and LLPs already have comprehensive documentation and tracking systems and supply-chain parties whose processes are not fully web-enabled will find themselves at a serious disadvantage in achieving full security compliance. A growing number of global shippers and intermediaries handling their own logistics are turning to multi-carrier portals such as GT Nexus, CargoSmart and Intra, which offer services such as ocean and rail shipment booking, scheduling and

tracking; customized management reports; e-mail notification and exception alerts; and cargo planning and order management.

***In Transit***

Single-party responsibility and asset control are particularly advantageous in maintaining the security of goods in transit. Shippers must begin to consider factors such as whether the containers used for its shipments have truly tamper-proof seals; whether ships might be registered under ‘flags of convenience’ with lax certification rules and employee screening for officers and crew; whether rail cars are dedicated or common user; whether truck operators are under contract, screen drivers and use driver teams for fewer stops; whether rail cars and trucks are fitted with GPS locator systems. Security gaps are less likely when control is centralized, with common standards applied under contract.

***In Facilities***

When it comes to security, port and inland terminals, container freight stations, transloading facilities, inland intermodal terminals, consolidation and distribution warehouses may all be among the weakest links in the supply chain.

It is at these facilities that cargo sits idle – and potentially vulnerable – the longest during a move (the potential for piracy or attack at sea is more limited). The following are among the questions that might reasonably be asked during any initial threat assessment:



- **Is the cargo being routed through ports, terminals and inland facilities with C-TPAT or equivalent certification?**
- **Does the shipper or LLP have ownership or contractual leverage over the facilities it uses?**
- **Are the perimeters of container storage areas secured with adequate fencing, surveillance and patrols?**
- **Is a designated security officer on the premises to supervise entry/exit of cargo?**
- **Are employees screened, and access restricted within the terminal according to job function?**
- **Are procedures in place for monitoring containers, verifying seals and, where cargo is loaded and unloaded, verifying contents, count and weight?**



- **Are procedures in place for reporting exceptions and suspicious activity?**
- **Are gates configured, with procedures in place, to prevent unauthorized entry and removal of cargo?**

Where supply chain productivity concerns itself with streamlining for speed and flexibility, security considerations focus on thoroughness.

As with normal supply-chain operations, contingency planning is also important. Handling, routing and scheduling flexibility must be built into the system to keep inventory moving and delivery commitments met in the event of inspection delays or an actual terrorist attack. This may include diversifying carriers, port gateways and/or regional distribution patterns under contract to ensure reliable, secure services and equipment if and when cargo flows must be quickly shifted.

Finally, there is a broader issue of turning container equipment more efficiently. Most terminals in the U.S. still operate on limited shifts, and there is an understanding that delays may occur in staging the container in the yard, or in scheduling a truck pickup. At times, shippers warehouse their cargo in the container, delaying pick-up and taking advantage of free time allowances before detention charges begin accruing. All parties in the supply chain will need to turn equipment more efficiently, in order to reduce costs, ensure equipment availability when needed and keep idle containers from becoming terrorist assets.



# 5: Conclusion

Security concerns demand a new layer of visibility in the supply chain. This can be a positive for shipper and LLP if handled properly, because it encourages far greater cooperation among parties, and an overall tightening of operations and information collection.

Many of the largest manufacturing shippers with complex or multiple supply chains and leverage with suppliers, logistics vendors and government, may opt to centralize and manage security functions internally. Other businesses are likely to seek out an LLP as a supply-chain manager, one that has been pre-cleared in its processes and eligible to move freight with minimal interruptions or delays for security inspections and audits.

Whichever option is pursued, a logistics division's or LLP's effectiveness will turn on the ability to bring the full range of transportation and logistics services under its control, link services and equipment with real-time information management and communications and apply common security standards throughout the chain with full audit capability.

Much groundwork for securing the supply chain from terrorism has already been done, whether as part of continuing improvements to supply chain efficiencies and value, or specific efforts to control narcotics or dual-use technology exports. It should not be assumed that security measures applied in the past to narcotics, or



dual-use medical equipment and computer exports, will necessarily produce the same results against terrorists with different strategies and delivery considerations, plus a willingness to give their lives in an operation. Yet it is also clear that industry and government are past the point where they need to reinvent the wheel.

Government will set the parameters for increased security, but industry will ultimately develop the technologies, systems and procedures for implementation. Security requirements must be coordinated and consistent across multiple borders, facilities and transportation modes in order to succeed.

Success in securing the supply chain relies less on new methods and technology than it does on greater cooperation and information sharing among supply-chain parties and between the public and private sectors. Clear, uniformly enforced strategies that build on existing commercial and government data at minimal cost and with minimal disruption to the flow of trade are essential to success. It's a tall order. And it brings costs with it. But success depends on it.

# Appendix A: Sources

*The following published materials were used in preparing this paper and are recommended to readers looking for more information on the topics covered.*

- Atkinson, Helen. "Untangling the Web." JOC Week, July 1-7, 2002, pp. 10-12.
- Benjamin, Mark. "Long Race to Safeguard Seaports." United Press International, February 8, 2002. [www.upi.com](http://www.upi.com).
- Caterinichia, Matt. "DOT Tests E-Seals on Shipments." Federal Computer Week, June 12, 2002. [www.fcw.com](http://www.fcw.com).
- Cottrell, Ken. "Security in the Spotlight." Traffic World Magazine, July 22, 2002, p. 33.
- "Customs-Trade Partnership Against Terrorism (C-TPAT) Security Recommendations." U.S. Customs Service, April 2002. [www.customs.usstrea.gov](http://www.customs.usstrea.gov).
- Dannas, Philip. "APL: Security Means 'Risk Profiling.'" American Shipper Magazine, May 2002, pp.22-23.
- Delaney, Robert V./Wilson, Rosalyn, "Managing Logistics in the Perfect Storm: the 12th Annual State of Logistics Report" (Summary). Cass Information Systems, Inc. June 2001, pp. 1-8.
- Dettmer, Jamie, "Tighter Security in Store for Seaports." Insight Magazine, February 25, 2002.
- Dupin, Chris, "The Dollars Start Flowing." JOC Week, June 24-30, 2002, pp. 30-31.
- Edmonson, Bob, "Cargo Security Puzzle." JOC Week, December 17-23, 2001, pp. 10-13.
- Edmonson, R.G. "The Cost of Cargo Security." JOC Week, August 12-18, 2002, pp. 10-12.
- "Existing Ocean Carrier Systems Considered in Security Push." American Shipper Online, June 25, 2002.
- Flynn, Stephen E., "America the Vulnerable." Foreign Affairs, Jan.-Feb. 2002, pp. 60-74.
- Gallagher, John, "Certifying the User." Traffic World Magazine, June 10, 2002, pp. 28-29.
- Hasson, Judy/Caterinichia, Matt. "Cargo Security on Agency Hit Lists." Federal Computer Week, June 24, 2002. [www.fcw.com](http://www.fcw.com).
- Hickey, Kathleen, "Radio Tags Too Pricey?" JOC Week, July 8-14, 2002, p. 46.
- Hickey, Kathleen, "Tag Master." Traffic World Magazine, July 8, 2002, pp. 18-19.
- "Improving Security for International Liner Shipping." World Shipping Council working paper, January 17, 2002.
- International Maritime Organization, "MSC Interessional Working Group on Maritime Security: 11-15 February 2002. IMO Newsroom, [www.imo.org](http://www.imo.org).
- Koch, Christopher, President and CEO, World Shipping Council. "Testimony before the Senate Committee on Commerce, Science and Transportation, Charleston, South Carolina," February 19, 2002.
- Kroft, Steve, "On the Waterfront." Transcript from 60 Minutes broadcast, March 24, 2002. Burrelle's Information Services.
- McLaughlin, John/Porter, Janet, "U.S. Tightens Grip on Box Security." Lloyd's List Online, August 9, 2002.
- Mongelluzzo, Bill, "Cost Uncertainty." Traffic World Magazine, June 17, 2002, p. 30.
- Mottley, Robert, "Security Quiz." American Shipper Magazine, July 2002, p.4.
- Seideman, Tony, "Security Measures Move into High Gear." Marine Digest, July 2002, p. 9.
- Simons, Marlise, "American Antiterror Inspections Will Begin at 3 European Ports." New York Times, June 30, 2002, p. 10.
- Speares, Sandra, "U.S. Security to Put Box Documents to the Test." Lloyd's List Online, August 9, 2002.
- "Technology Systems Expand at Box Terminals." Marine Digest, June 2002, p. 17.
- Thorby, Chris, "Filling the Voids." Containerisation International, July 2002, p. 51.
- "U.S. DOT Announces Successful Test of Cargo Technology." Associated Press, June 5, 2002.
- van der Jagt, Nicolette, "Familiarity Breeds Security." Containerisation International, June 2002, p. 37.
- Villalon, Bill, President for the Americas, APL Logistics. Presentation before the National Retail Federation 91st Annual Convention, New York City, January 15, 2002.
- "WCO Adopts Resolution to Improve Global Supply Chain Security." American Shipper Online, July 2, 2002.
- "When Trade and Security Clash." Economist, April 6, 2002, pp. 59-62.

# About APL/APL Logistics

*This paper was prepared by APL and APL Logistics to help their customers, employees and the broader public better understand the scope of security issues involved in container transportation and supply-chain management, and the effort required to address those issues.*

**APL** is an integrated container transportation company that provides end-to-end freight transportation services around the world. Through its network of more than 90 ships, eight ocean and inland terminals, around 200 offices in some 87 countries, around 450,000 containers and chassis, plus its preferential rail and truck partnerships and state-of-the-art information technology systems – APL offers more than 60 weekly services and nearly 300 calls at over 90 ports in Asia, Europe, the Middle East and North America. APL serves all major cities and manufacturing centers in Canada and Mexico, in most cases with in-bond shipment capability to speed entry at border crossings. It offers special advantages in the China market where it has operated since 1867, with more than 30 offices; direct calls at Shanghai, Qingdao and Yantian as well as Hong Kong; and extensive intermodal connections to interior points.

**APL Logistics** provides full end-to-end logistics and supply-chain management services through its 4,700 employees, 200 warehouses and 115 offices in more than 55 countries. APL provides customers with the full range of value-added global supply chain services, including planning and analysis; contract logistics and warehousing; facilities management; consolidation and vendor services; global freight transportation; IT

solutions; and overall supply-chain management as a lead logistics provider. Among third-party providers, APL has led the industry in electronic transmission and receipt of purchase orders (PO) and Advance Ship Notices (ASN), and was first to offer a PO/shipment tracking application on the Internet. APL specializes in systems and services that integrate end-to-end supply-chain shipment data from multiple sources, in customized reporting and documentation. Its latest innovation, APL Logistics See Change Services, is a data connectivity, monitoring and adaptive response tool that provides a flexible way for companies to proactively monitor and respond to exceptions with one of four solutions: expediting, diverting, re-sourcing or substituting product, thus optimizing control and inventory management.

APL and APL Logistics both have a history of close cooperation with the U.S. Customs Service, initiating and participating in pilot programs aimed at making Customs processes more efficient while streamlining cargo clearance and inspection. Among its accomplishments, APL provided technical and operational support in testing and developing the USCS Automated Commercial System (ACS), which enables importers and logistics providers to file customs documents electronically; and implementation of in-bond shipments, to eliminate port

terminal congestion and delays by processing pre-screened cargo at its inland destination. APL has also been a key participant in government programs to address smuggling of narcotics and illegal aliens, and in the safe handling and transport of hazardous cargoes.

**Both APL and APL Logistics are subsidiaries of Singapore-based Neptune Orient Lines (NOL).**

# At a Glance: Securing the Supply Chain

(-TPAT security compliance will become an increasingly critical supply chain component in coming months. It will determine the extent to which shippers and their logistics providers may encounter U.S. Customs inspections, audits and other potential interruptions to inventory flow over time.

Even supply chain partners not directly included in (-TPAT will come under growing pressures to meet compliance targets from partners who are in the program. Below is a checklist of questions all parties in a supply chain should be asking themselves and each other in moving forward with their compliance initiatives:

## Facilities

- Are buildings constructed of materials resistant to unlawful entry and intrusion?
- Are outside and inside facility doors, windows, gates and fences adequately locked?
- Are international, domestic, high-value and dangerous cargoes marked and segregated in distinct, secured areas within the warehouse?
- Is each facility adequately lighted inside and out, including parking areas?
- Is private vehicle parking kept separate from shipping, loading dock and cargo areas?
- Are gates under surveillance by security/management personnel?
- Are alarm and communications systems in place to alert internal security or local police?

## Access

- Is access to shipping, loading dock and cargo areas restricted by clear, enforced procedures (identification, logging and tracking of all employees, visitors and vendors)?
- Are procedures in place for challenging unauthorized/unidentified persons, including requirement of searches?
- Are vehicles, containers and other conveyances routinely moving into, out of and within accessible areas regularly checked for unauthorized personnel, materials or signs of tampering, with procedures for reporting irregularities?
- Are vessels, aircraft and rail cars secured from unauthorized boarding, with accessible alarm systems and procedures in place for alerting internal or external security personnel?

## Procedures

- Does a designated security officer supervise introduction/removal of all cargo?
- Is inventory fully and properly marked, weighed, counted and documented, and then verified?
- Are procedures in place for affixing, replacing, recording, tracking and verifying seals on containers, trailers and rail cars throughout the move?
- Are procedures in place for detecting and reporting shortages and overages?
- Are procedures in place to track the timely movement of incoming/outgoing goods?
- Are empty and full containers stored properly to prevent unauthorized access?
- Are empty containers examined upon receipt?
- Is hazardous cargo properly labeled and stored separately?
- Is there a container loading verification procedure to screen for unmanifested containers?
- Are procedures in place to notify Customs and law enforcement agencies of irregularities or suspected illegal activity?

## Personnel

- Are employees adequately screened and interviewed before hiring, including background checks and application verification?
- Are employees restricted in their access to shipping, loading dock and cargo areas by specific job classification and function?

## Education and Training

- Is a security awareness program in place that educates employees in recognizing suspicious activities, maintaining product/cargo integrity and determining and addressing unauthorized access?
- Is there an incentive program in place for active employee participation?
- Are internal security audits conducted?

## Documentation

- Are shipping documents complete, legible and protected against exchange, loss or inclusion of false information?
- Are procedures in place for verifying accuracy of basic information such as shipper and consignee names and addresses, first and second notify parties, and cargo description, weight, quantity and unit of measure?
- Are procedures in place for reporting/investigating documentation discrepancies, including inventory shortages or overages?
- Are procedures in place for tracking movement of incoming and outgoing goods?
- Is computer access to shipment information adequately safeguarded?
- Is manifest information complete, legible, accurate and submitted on time to Customs?