

Speech by Earl Agron,
Director, Port and Container Security, APL

**“Balancing Business Costs, Opportunities and
Efficiencies versus Security”**

Presented at the Asia-Pacific Maritime Summit 2004
Singapore Expo, Thursday, 25 March 2004

Balancing security with the free flow of goods was an objective at APL long before September 11. Back then, we focused on preventing damage and theft.

Now, the focus also emphasizes the prevention of terrorism. But the goal is the same: To provide strong security while still allowing our customers' supply chains to flow freely and efficiently.

I'd like to talk today about four aspects of security.

The first is the **regulatory** aspect, and the importance of international cooperation in developing harmonized, global requirements.

The second consideration is the **ports**— will worldwide regulations create two classes of ports...those that comply with international requirements and those that do not?

The third is **technology** – what role can technology play in securing the supply chain?

And fourth and final aspect I will address is **cost**— who pays for all this?

Let's start with the regulatory aspect. When we concerned ourselves only with damage and theft, the primary stakeholders were our customers and ourselves.

Now ... following September 11th, the stakeholders also include the citizens of the world, and the governments that represent them.

With the entry of governments, we suddenly had regulations such as the United States Container Security Initiative also known as CSI, and its centerpiece, the Advance Manifest Rule. And now, we have ISPS – the International Ship and Port Facility Security Code, adopted by the International Maritime Organization.

People often ask me if APL has gained efficiencies from implementing governmental regulations such as the Advance Manifest Rule. Likewise, I'm asked if we have benefited from our voluntary participation in the US Customs-Trade Partnership Against Terrorism, known as C-TPAT.

In both cases, the answer is, “yes ... but participation is not without cost.”

The Advance Manifest Rule, often called the “24-Hour Rule,” requires numerous data elements about a shipment to be communicated to US Customs and Border Protection at least 24 hours before a vessel sails. In comparison, before the advance manifest rule, we had until the ship was just two days away from the US before more general information was required.

To comply with the Advance Manifest Rule, we had to re-program many of our systems and change our work processes.

We basically took our best operating personnel, business analysts and software developers and put them to work on the project for two solid months.

The cost of this initiative was not only the direct costs of our IT folks; it was the opportunity cost of diverting resources away from other very important efforts.

The benefit is that we now have all the shipment information before sailing. That helps us plan our vessel and terminal operations more efficiently than in the past.

It has also allowed us to dramatically reduce the amount of rework our documentation staff needed to deal with. Prior to the Advance Manifest Rule, 75% of all manifests needed some adjustments. Today that number has been reduced by over half and we expect even more improvements through time.

When the Advance Manifest Rule went into effect a year ago February, we anticipated that hundreds of containers might be held by Customs. A little more than a year later, I’m pleased to say that cargo holds, in general have been minimal. I understand that out of 12 million bills of lading only 1% received “DO NOT LOAD” orders because of the information filed.

In fact, I have not heard of one APL container missing its intended ship because of the Advance Manifest Rule. Our customers are doing an excellent job of providing the data that Customs requires. And that has led to a program that has provided security with very little impact on the flow of goods.

Beyond the Advance Manifest Rule, what are the requirements of the Container Security Initiative or CSI? First, a potential CSI country must have a substantial volume of containers moving to the US. Given that, here are the 5 basic requirements as spelled out by US Customs:

- 1) Local authority to inspect containers
- 2) Availability of inspection equipment
- 3) An established risk-management system
- 4) Willingness and ability to share critical data with US Customs and Border Protection

5) Ability to identify breaches in cargo integrity

The cost of CSI comes mainly from investment in x-ray, gamma-ray or radiation detection equipment. And there are some additional personnel expenses to operate the equipment.

For a medium to small location, assuming one or two gamma-ray inspection machines, the total cost would be less than US\$5 million.

CSI initially has focused on the top 20 ports that represent approximately 67% of US imports. For smaller and medium-sized ports who find such investment somewhat challenging they may look to their governments for support to meet the standards.

And this should be a priority.

According to US Customs, CSI deters terrorist organizations that may be seeking to target ports.

If terrorists were to use a cargo container to carry out an attack on a seaport, the maritime trading system would likely come to a halt until security was improved. US Customs currently says that CSI ports would be able to resume trading with the US sooner than others. So, in short, you could look at CSI as a relatively inexpensive insurance policy in the event of an attack.

Now APL is also certified and verified under the guidelines of C-TPAT – the Customs-Trade Partnership Against Terrorism. And we have seen both tangible and intangible benefits.

One of the bigger benefits of C-TPAT has been an intangible –we now have a new framework for our business. That framework is security. C-TPAT has raised the level of security awareness up and down our organization and those of many of our customers and vendors.

So, yes – CSI and C-TPAT both provide benefits. But here, we're talking just about US regulations.

Last month, in my email box I had individual messages about changes to the US Advance Manifest Rule, as well as manifest requirements of Australia, Peru, Canada, India and Panama. And then we have to think about what is over the horizon in Europe and other regions.

Keep in mind that one country's imports are another country's exports, and still other countries' in-transit and transshipment boxes.

Each nation naturally wants to protect itself, and so issues regulations about container security. The danger is, that without harmonizing those regulations, we will all get lost in a maze of administrative requirements.

That carries two risks. First, we have the possibility of accomplishing what the terrorists of September eleventh may never have imagined. Out of our fear of a repeat attack, we will have misallocated our priorities and our resources to the point that world trade could reach a virtual standstill. Second ... we can get so involved in meeting the requirements that we take our eyes off the ball and miss the terrorist threat when it actually comes.

How can we prevent that?

I would like to challenge the members of the World Customs Organization to roll up their sleeves and become THE FOCAL POINT on container security, in the same way that the IMO has taken on ship and port security with ISPS.

I know this task isn't easy but it is an important one.

With the adoption of ISPS, we will have international regulations for vessels and ports in place by July first of this year. ISPS represents a real success story. All trading nations have signed up to a standardized code and a time frame for implementation. All signatories are supposed to honor the certifications from other nations.

By the way, APL has recently become one of the first companies to have its entire owned fleet certified under ISPS. That involves thirty-one vessels. It is the result of the excellent work of our fleet management company, Neptune Ship Management Services and our company's commitment to security and the uninterrupted flow of our customers cargo.

Is **ISPS** perfect? Probably not. But it is a step to coordinate our efforts. ISPS represents a consistent and uniform approach to security, and provides a good model for other security initiatives.

Reaching worldwide compliance by this July presents a considerable challenge. Some 50,000 vessels and over 1,500 port facilities globally need to secure certification. It does seem clear that not all parties will be compliant in just a few months.

It also seems clear that the US, at least, will more than likely deny entry of non-compliant vessels after July 1st. The big question is really what will happen when a compliant vessel arrives at a compliant port, but has previously called someplace that is not in compliance. The consequences are still being considered. It is very important that this question be cleared up immediately to

allow carriers to build back-up plans based on a well defined set of consequences.

Let's move to the topic of technology.

When you say security, it seems to exert a gravitational pull that attracts an array of vendors with their gadgets and gizmos. The problem is that when it comes to security:

Process ... people ... and training ... are equally important.

In fact, a great deal of the technology I hear about has little to do with security. It really has more to do with supply-chain management. Of course, by using security as the sales pitch, the vendors hope we won't bother to justify the purchase of their gadgets solely based on the benefits of improved supply-chain visibility.

So let me ask the question: Does greater visibility, in and of itself, always provide the kind of security we're looking for? .

There are four aspects that come into consideration here.

- First, different types of visibility provide different levels of security.
- Second, at a certain point, lots of visibility becomes difficult to manage. We have to ask the question, "How much is enough?"
- Third, certain types of visibility simply overlap what we already have. Do we really need them? Do they add value?
- And, fourth, we receive only so much marginal return in real security for our investment in visibility. How can we discern between security benefits that we ought to have, and other benefits that might simply be nice to have?

For example: If you put Radio Frequency Identification (RFID) tags on products, on cartons, on shipping labels, on pallets, AND if you enter detailed cargo manifest information on electronic seals, you can know almost everything about what is moving in the container at any given time.

BUT – so can the bad guys.

Wait, you say ... the experts have already considered cyber security ... We can assume it's completely secure.

Personally, that seems to me to be a giant leap of faith to assume cyber security has no problems.

Let's look at GPS as an example.

According to one of the United States National Research Laboratories, GPS signals are easy to counterfeit. A bad guy can easily fool a GPS container-tracking system by feeding the GPS receiver fake signals so that it looks like it's somewhere where it's not.

For now, let's put that aside, and talk about potential benefits of GPS. It is indeed a popular idea is to attach some type of GPS gadget to each and every container moving around the globe so we can follow each box through its journey along the supply chain.

BUT – let's be careful ... Let's balance the cost of tracking the containers on a real-time basis against the incremental benefit of HAVING that real-time access.

Today, most ocean carriers can locate their containers within a reasonable amount of time WITHOUT GPS.

For example, when containers are on ships, trains or in marine terminals, the location data is already captured in our proprietary systems.

With just a few keystrokes, we can tell you where those containers are located. And the safeguards against hackers are quite mature.

If a container has been dispatched for stuffing, generally we know who picked up the container and when it's expected back at the marine terminal.

If, for some reason, the authorities need to "capture" that container, then we have the ability to "trap" it when it returns to the marine gate before being loaded onto a ship.

So one might ask if there is a more efficient and economic means of tracking containers other than outfitting every container on the planet with GPS.

For example, you might consider GPS tags on just the truck cab or the chassis for inbound loads over the road. That's the segment of the supply chain where visibility could be further enhanced with GPS tags.

This would dramatically reduce the number of tags you would need and the underlying expense. Of course, vendors selling this service will doubtless offer a different perspective.

Now when it comes to container visibility in the supply chain, the ultimate is the so-called smart container.

Actually there is no official definition of a smart container.

I have seen definitions that include capabilities for sensing explosives, radiological devices, chemicals, biological agents, human presence, intrusion detection, location, and so on.

When we talk about all of these capabilities, we really need to ask: “What are the vulnerabilities that need to be sensed, AND is the inside of the container the most efficient and COST-effective place to do it?”

In my opinion, many vulnerabilities can be more economically and effectively screened landside, rather than inside the container.

Retrofitting approximately 12 to 15 million legacy containers with sensors that are robust enough to withstand the rigors of our business is just mind-boggling.

Also, one must keep in mind the management of the mountains of data generated by the so-called smart container.

- Which party should receive the signal?
- Who has custody of the container?
- How do you identify false positives?
- How do you handle nuisance alarms?

Remember, if 10 million smart containers send out a signal only once every hour, we would have to process almost a quarter of a billion messages each day. The danger is that we make the haystack so large that we can't find that needle we're all looking for.

Another popular topic of conversation is the electronic seal. Electronic seals have **NOT** been proven to provide significantly more security than the cheaper high security bolt seals. Also, **NO** single radio frequency has been identified for electronic seals that works worldwide at this time.

However, carriers and shippers may want to still consider the option of using electronic seals in order to perform seal checks and/or improve visibility.

If electronic seals ARE introduced, I suggest five guidelines. They are the recommendations of the recent In-Transit Security White Paper distributed by the World Shipping Council, the International Mass Retailers' Association and the National Industrial Transportation League.

- 1) The electronic seals should have a unique number that can be read both electronically and manually.
- 2) The electronic seal should record only the date and time it was activated AND the date and time it was opened or breached.
- 3) Operation should be within a single radio frequency available worldwide, and able to be read by a universal reader.

- 4) The electronic seal must perform reliably.
- 5) The seal must meet minimum physical security standards of the ISO .

Finally, before we begin investing millions of dollars in technology, let's make sure we have effective industry processes and procedures.

Here are four responsibilities recommended in the In-Transit Security white paper.

- 1) It is the shipper's responsibility for sealing the container upon stuffing.
- 2) Any seal changes must be reported to all involved, and entered into appropriate systems.
- 3) The party receiving the container must verify and record the seal number and its condition.
- 4) No container should be loaded without having a high-security seal affixed.

Again, as I mentioned: people, processes and training are equally important as any technology that we might choose to apply.

On to my fourth and final topic: **Cost**.

When it comes to cost, protecting against terrorism is really an unfair fight.

The bad guys, with a relatively modest investment, can inflict massive physical and economic harm not to just our industry, but to society at large.

At the same time, the cost of mobilizing our industry against terrorism can be staggering. That's why, regardless of who pays, we all have to ensure that we get the highest possible return on each security dollar invested.

Can we really make world trade secure without breaking the bank or without slowing down the supply chain velocity?

First, there's the sheer volume of cargo. Roughly 20,000 containers enter the United States each day. And far more enter all of the other countries of the world.

Some suggest 100% inspection of containers.

Even if that were possible (which is another story), not only would you have to inspect every container but would have to open every package in every container and then hope that the inspector is well-trained enough to recognize the bomb or weapon.

Remember there will be no packing slip that says BOMB inside.

The Brookings Institute says it could cost more than \$50 billion a year for a completely comprehensive, worldwide system of inspection. It also says the cost of delaying the delivery of imported goods by a single day could amount to an additional \$7 billion a year. And these costs only refer to the US economy and exclude similar impacts to the rest of the world.

CLEARLY, THE COSTS ARE TOO GREAT TO HAVE 100% INSPECTION.

Thus far, the cost of improving security in ocean shipping has been borne mainly by the our industry. That would be fair if we were protecting only our cargo and ourselves, as we were doing before 9-11.

But the cost of a terrorist attack is spread throughout our society. Thus, it's fair to suggest that the cost of PREVENTING an attack also be spread throughout the society at large. Clearly, government has a critical role here. I believe that role is to work with industry to help sort through the issues and arrive at solutions that are rational, equitable and universal.

As I've emphasized, the greatest potential cost is the restriction of international commerce. So, above all, our approaches to security must allow trade to continue flowing freely. Otherwise, we may succeed in combating terrorism, only to find that we, and not the terrorists, have crippled the global economic system on which we all depend.

Allowing a free flow of trade relies on one thing: Complete cooperation among the trading nations of the world.

As with the embrace of ISPS, the nations must also come together to create universally accepted requirements for container security. Only then can we be certain that international trade can flow both securely and efficiently.

A conference such as this one is the right place to raise the issue. But what we must have, and have soon, is concrete action toward making such standardized regulations a reality in this new era for global maritime trade.

Once again, I offer the challenge to the World Customs Organization and respectfully urge them to take the lead in this endeavour.

It is my sincere hope that in the not too distant future, we will begin to see the emergence of global harmonized regulatory security requirements.

Without this, we may face a tangle of regulations that can slow global trade and focus us on administrative details instead of thwarting the bad guys.

With harmonized regulations, we can help world trade continue to move efficiently while we all remain vigilant against the threat of terrorism.