



WORLD SHIPPING COUNCIL
PARTNERS IN AMERICA'S TRADE

Remarks of
Christopher Koch

President & CEO of the
World Shipping Council

Before the

**Journal of Commerce's
4th Annual Trans-Pacific Maritime Conference**

**Long Beach, California
March 9, 2004**

It is a pleasure to address the 4th Annual Trans-Pacific Maritime Conference in order to discuss container security initiatives and some of the issues that shippers and carriers can expect to see in 2004. The last eighteen months have seen significant initiatives by the government, working with industry, to enhance the security of international maritime commerce. 2004 will involve more changes – some from implementation of regulatory regimes that were developed last year, and some from new initiatives. Taking security enhancement to the next level will be a key priority for the Department of Homeland Security this year.

Before addressing the specific issues, however, I would like to recognize the extensive efforts of the many people in the Department of Homeland Security's agencies that are working every day to enhance security, while not significantly disrupting commerce. This is difficult and complicated stuff. The answers regarding how best to address these issues are not obvious or simple. But progress is clearly being made, and we should recognize the efforts that our public officials are making every day to continue to improve security policies and programs. There will be times when industry sectors

may have a different perspective on the best way to address an issue, but officials in the Department of Homeland Security are doing their best to deal with a challenge of immense scope, and we appreciate the fact that they are doing so in consultation with industry shareholders and other governments.

1. Vessel and Port Security

Because of the nature of this conference and its focus on how trade and cargo flows will be affected by the new security initiatives, I will not dwell on the details of the substantial efforts that vessel operators, terminal operators, and ports are expending to comply with the July 1st effective date of the new vessel and port security plan regulations. These regulations were established by the Coast Guard to implement the requirements of the Maritime Transportation Security Act (MTSA) and the IMO International Ship and Port Facility Security Code (ISPS).

There is a substantial amount of work that must be done to be compliant by July 1st. Discussions with our Member lines' representatives have identified no significant problems regarding lines' expectations of their vessels being compliant by that time. Furthermore, we are unaware of any U.S. container terminals that do not plan on being compliant by that date.

It would appear likely, however, that not all foreign port facilities will be compliant on July 1st. This may be of particular concern in some developing countries. It seems clear that the U.S. will not stop trade with such countries in July; however, the issue is how will ISPS compliant vessels be treated by the U.S. Coast Guard and other nations when they arrive after having called at a foreign port facility that does not have an ISPS compliant facility security plan. Vessels calling between such ports and the cargo on those vessels are caught in the middle. It is not yet clear what a vessel can expect in these situations.

Shippers too should expect consequences to cargo that passes through noncompliant facilities, and those consequences may become more substantial as time passes and the government becomes less tolerant of foreign ports that are not compliant with the Code. For example, it is possible that Customs' Automated Targeting System may assign a higher security risk to cargo containers transiting through non-ISPS Code compliant facilities, and thus make it more likely such containers will be held up for inspection. While the government may be highly reluctant to stop trade with such countries, it is likely to undertake measures designed to impose pressure on such ports and governments to comply. Once the Coast Guard undertakes, in coordination with other governments, foreign port security assessments as required under the MTSA, it may be in a better position to identify any particular ports of concern. In short, the U.S. and other ISPS Code compliant nations are likely to take actions that will cause carriers and shippers to have a common interest in strongly supporting efforts by all countries to become compliant as soon as possible.

2. Cargo Screening and the Automated Targeting System

As you all know well, soon after September 11, U.S. Customs developed and implemented a strategy to enhance the security of containerized cargo by: 1) requiring the industry to provide the agency with advance cargo manifest information 24 hours before vessel loading in a foreign port, 2) having such information analyzed by the agency's Automated Targeting System (ATS), and 3) inspecting any container about which ATS raised significant questions. ATS is thus a central factor in determining which containers get inspected and in the working relationships that Customs is establishing with other trading nations' Customs administrations.

It is noteworthy that with international liner shipping, unlike the other transportation modes, the government strategy is to perform cargo security screening before the cargo is loaded onto the transportation conveyance coming to the U.S. The 24 Hour Rule has been implemented without major incident, and Customs has worked closely and cooperatively with industry to address those issues that did arise, such as the NVOCC special bills of lading. The Rule's importance is obvious to the security strategy described, and ocean carriers have supported Customs' initiative and the Rule.

While today ATS is populated with carriers' bill of lading data, a significant question to be addressed in 2004 is whether these bill of lading data elements are sufficient for the security task at hand. Earlier this year the complexities of this issue became obvious in the context of the Trade Act's cargo shipment documentation regulations. Customs amended the cargo manifest regulations' treatment of who the carrier should name as the "shipper" on its bills of lading that are filed with the agency, out of a desire to capture information about the identity of an importer's "foreign vendor, supplier, manufacturer, or other similar party". I will not repeat all the issues created by this proposal. For those who want to read the 28 pages petition we submitted to Customs on this issue on February 2, the document can be found on the Council's website.¹

What is clear at this point is that the agency recognized the problem that the regulations created, suspended enforcement of that portion of the regulations, and announced that it would work with the industry to review these issues. In short, it acted in a most professional and responsible manner. What remains to be addressed, however, are some hard issues. While it appears clear that information about importers' "vendors, suppliers, and manufacturers" is not appropriately obtained by trying to change who should appear as a "shipper" on a transportation contract – a bill of lading, it is not so readily apparent how such information is best obtained by Customs if it is to be used in the ATS for security screening before vessel loading in a foreign port.

Because this is an important issue that is likely to be addressed this year, I would like to offer some preliminary observations.

One should start by recalling the terms of the law. Section 343 of the Trade Act requires:

¹ www.worldshipping.org

“In general, the requirement to provide particular information shall be imposed on the party most likely to have direct knowledge of that information. Where requiring information from the party with direct knowledge of that information is not practicable, the regulation shall take into account how, under ordinary commercial practices, information is acquired by the party on which the requirement is imposed, and whether and how such party is able to verify the information.”

In short, the information of interest – an importer’s vendors, suppliers or manufacturers – is clearly information within the “direct knowledge” of the importer, not the carrier. In fact, the importer today provides this information to Customs in an existing Customs data system in the merchandise entry process. The difficulty is that this information is not currently filed before vessel loading in time to be useful to ATS.

When Customs wanted carriers’ manifest information earlier than the formerly required time of vessel arrival at the U.S. port, the government established the 24 Hour Rule and required carriers to change their systems and processes to comply. The same logic might be applied by requiring shippers to provide Customs with their data before vessel loading. Although shippers may not relish the idea of doing so, such a process is used for U.S. export cargo.

The threshold issue is whether Customs needs the information about an importer’s suppliers and vendors before vessel loading in order for ATS to become more effective. There is in fact an over-arching and broader question that underlies this issue and the effort to make ATS as effective a cargo security screening system as possible, namely: What information does the government need, from whom, when, filed into what information system? Clarity and agreement on this important fundamental question will be important to understanding what gaps exist, what the objectives are, and how we can all determine how best to make the continued progress we all recognize is desired.

The Trade Act regulations make it appear probable that shippers are going to be involved in measures to provide the government and the ATS more advance information about their cargo shipments before vessel loading. It is also reasonably certain that carriers are unlikely to want to be made into conduits for transmitting to the government information they don’t know, cannot verify, and could be penalized for if inaccurate.

In addition to the language of the Trade Act that indicates carriers should not be the parties filing this information, there are other aspects of this issue that all sectors of the industry will need to consider. First, there is the issue of confidentiality. Do shippers want their supplier and vendor lists given to carriers, and filed in the public manifest system? Second, early carrier manifest filings with Customs administrations are becoming more prevalent around the world. For example, Panama will soon be implementing an advance cargo manifest filing system very similar to U.S. Customs’ system for every container transiting the Canal, regardless of whether Panama is the cargo’s origin or destination. The measures taken here in the U.S. on this issue could easily become a precedent for other nations. Do shippers want their supplier and vendor

lists broadly distributed via carrier manifests? Third, would such requirements apply to foreign-to-foreign cargo shipments that move on ships that call U.S. ports or are relayed in bond through U.S. ports? Because it is highly unlikely, for example, that a European importer of Latin American goods is going to supply the U.S. government with a list of its vendors and suppliers just because the ship calls at the Port of Miami, such a measure applied to such goods could have a substantial effect on vessel deployments, vessel calls at U.S. ports, and other service related issues.

In short, Customs has addressed the immediate problem that existed in the drafting of the existing Trade Act regulations, but the agency and the industry have yet to determine how the underlying issues will be addressed.

3. Container Inspections

Today, Customs uses the ATS system to screen 100% of all containers before they are loaded aboard a vessel bound for the U.S. As it has refined ATS, ocean container inspection rates have increased, from less than 2% before September 11th to 5.4% according to the most recent reports. That means that Customs is now inspecting almost 400,000 ocean containers a year. We expect container inspections to continue to increase in 2004.

First, Customs has stated that its goal is to establish radiation-screening portals that will perform radiation screening on every container transiting U.S. ports. The implementation of this will be challenging, including addressing the screening of containers that are loaded onto on-dock rail cars and do not pass through the terminal gate, but the goal is clear and appears logical. Representative Nancy Pelosi, the Democratic Leader in the House of Representatives, has clarified that this is exactly what was intended in the Democrats' response to the President's State of the Union message in which she called for 100% container inspection. As a result, there does not appear to be any partisan difference of opinion on the objective, but we expect that Congress is likely to make probing inquiries of the implementation schedule for this program. We also note that foreign ports are undertaking similar measures to protect international commerce and that the Port of Rotterdam is implementing a similar radiation screening system.

Secondly, as noted, currently approximately 5.4% of all inbound ocean containers are inspected using non-intrusive technology or are physically searched. As Customs further implements its C-TPAT program, and as it refines ATS, it is likely that this number will increase. While some have projected that Customs' inspection rate may grow to 10%, we believe that a numerical objective should not be the goal. The goal should be to inspect 100% of all containers that ATS says warrant inspection, plus some random process designed to monitor and verify the selectivity techniques being used. How many of these inspections will be performed at U.S. ports and how many at foreign ports of loading we cannot tell at this time.

4. Container Security Initiative

I began these remarks discussing the Coast Guard's implementation of the new vessel and port facility security plan requirements, which the agency was instrumental in creating at the International Maritime Organization. The Coast Guard's strategy and its execution, as well as its communication and efforts working with the industry, have been excellent.

Customs, on the other hand, has not had the benefit of a comparable international regulatory organization to work with, so Commissioner Bonner and his organization have worked with Customs administrations in other trading nations to develop the Container Security Initiative – a set of bilateral agreements designed to foster closer cooperation and more effective security screening of international commerce. It is also significant that the Department of Homeland Security has reached an agreement with the European Commission that can promote trans-Atlantic cooperation and coordination of container security initiatives in conformity with the CSI approach and objective. We welcome this development. The importance of CSI should not be underestimated. Protecting international trade requires international cooperation. The World Shipping Council hopes that all participating governments will implement these CSI agreements effectively and cooperatively. Of the 38 CSI ports, 17 are currently operational.

The Congress has recognized the value and importance of CSI, but it is likely that in their oversight role, the House and Senate Committees of jurisdiction will be inquiring into various questions, such as: when are the non-operational CSI ports going to become operational, what other governments will be joining this initiative, are the governments deploying sufficient container inspection equipment, are they inspecting the containers CBP is requesting to be inspected, is there a cooperative sharing of intelligence, what happens if cooperation is not sufficient, what are the consequences of a failure to implement the agreements.

CBP deserves a lot of credit for where it has taken this initiative, which is still in its developmental stage. Ocean carriers are fully supportive of these initiatives, and we believe shippers will be too. In the event governments need to respond to a terrorist event in this industry, it is difficult to see how trade would not be irreparably harmed if CSI agreements are not operational and well implemented.

5. Technology and “Smart” Containers

As discussed earlier, technology is being improved and deployed more extensively to enhance container security through non-intrusive container inspection technologies and through radiation detection.

Government and industry also continue to examine technology that may be appropriate for application to containers themselves. Operation Safe Commerce continues to fund projects reviewing such possibilities. Customs and the Department of

Energy continue to review these issues, as do technology manufacturers, shippers and carriers.

As Commissioner Bonner has stated, the objective of this exercise is to make sure that containers are effectively sealed and that one can reliably detect if they have been tampered with in transit.

The “sealing” portion of this exercise does not really involve sophisticated technology. It requires shippers to seal a container immediately upon securely stuffing the box with a high security seal. E-seals do not provide any more security in this regard than a high security manual seal, but they may have a role in enabling a more efficient way to verify seal integrity.

E-seals involve the application of Radio Frequency Identification (RFID) technology, and in fact many of the products and platforms being marketed as enhancing container security also rely on that technology. Recent announcements by the Department of Defense and major retailers concerning the usage of RFID tags on products have also spurred significant interest in the technology.

It is important to keep in mind, however, that no international standard exist today for the application of RFID-based e-seals or for active, read/write RFID tags. Nor has a clear and appropriate delineation been drawn between the possible usage of RFID technology to address container security requirements and the possible usage of that technology to address supply chain management objectives. These are not trivial issues. The issues, the challenges, and the requirements involved in addressing the two are not the same. The purposes and the use are not the same. The technology, operational and information implications are different. A failure to clearly distinguish between security requirements and commercial supply chain management objectives will create confusion; will impede progress on these issues; and may in fact create significant security vulnerabilities.

There is also the issue of selection of frequency or frequency bandwidth. It simply would make no sense to select a radio frequency for RFID platforms that is not publicly available in all major trading nations. And it would be of little value to the government and industry if the frequency that is eventually selected would be deficient in terms of operational characteristics, such as requiring line of site to be read, producing false positives, etc.

The WSC is actively participating in International Standardization Organization (ISO) working groups tasked with the developing standards for RFID e-seals and tags. In fact, later this week we will be submitting several papers to the ISO, identifying user requirements for e-seals and a proposed Framework for the optional usage of RFID e-seals and tags.

We have also presented this Framework to CBP in response to its Request For Information (RFI) for “Smart and Secure Containers”. We commend CBP for having reached out to affected parties to solicit their input in this first stage of what we hope will

be a comprehensive and coordinated analysis of the issues involved in trying to identify technology's role in enhancing container security.

One of the more important and difficult issues in this regard is understanding and analyzing the information infrastructure and systems issues necessary to support a technology, whether RFID, wireless or satellites based, including:

- What information is generated, who is authorized to generate it, and is that information necessary for security purposes
- Who collects the information
- What supporting infrastructure the technology requires, where must it be located, and who operates it
- Who has access to the information
- What is done with the information
- What actions are to be taken, by whom, with respect to the information
- What are the costs of the technology and its use, and who incurs them, and
- How the technology may affect the operations of shippers, carriers, and the relevant government agencies?

The deployment of any such technology would involve many international supply chains, international operating systems, the need for cooperation in other national jurisdictions, and substantial costs. Consequently, it is essential that government and industry carefully and openly analyze all the issues to be sure that appropriate and clearly understood requirements are being defined and met, and that the requirements and technology are not going to be replaced and the necessary capital wasted in efforts to implement technology that is really not the best approach to the issue.

For example, there is the issue of how sensors might be applied. It is questionable to what extent and under what circumstances a sensor that only detects if the container doors have been opened would provide more useful information than a seal. Clarity is also needed on what must be sensed, and where. Is sensing more appropriately done at the port of loading through centrally operated sensing devices (as is done for radiation detection as discussed earlier) rather than equipping the world's 16 plus million sea containers with individual sensors? For devices installed on containers, there is also the issue of what kind of reading and information infrastructure is needed for these devices to work.

For example, some question RFID-based technology platforms for container security application because of their dependence on an array of ground based readers at multiple yet-to-be defined points in many facilities, in many different countries, controlled by many different parties. Increasingly such RFID skeptics question whether satellite and/or wireless technologies are a potentially superior way than RFID-based technology to address security requirements as they are developed. We do not yet know the answer, but these issues need to be addressed before decisions are made on the deployment of technologies, which – as I mentioned – will have significant cost and operational

implications for customs administrations, shippers, carriers, and terminal operators around the world.

Undersecretary Hutchinson recently announced a significant and important change in the Department of Homeland Security. Responsibility for the issues of smart and secure container technology and systems has been moved from the Transportation Security Administration to the Border and Transportation Security Directorate, with Customs having a major role in implementation and with TSA having an advisory role. The issue, in short, has been moved “upstairs”, and a new consultative process with the industry announced to help address the issues involved.

It is not entirely clear how the ongoing “smart” container analysis within Customs will be integrated into this process, but it presumably will be. Customs, like Operation Safe Commerce administered by TSA, has been conducting tests of some technologies, and there has been discussion about whether the Customs Trade Partnership Against Terrorism would be used as an implementing mechanism for “smart” boxes. The World Shipping Council members certainly view these issues as requiring a close and transparent working relationship between government and industry if they are to be successful. We also note that section 102(d) of the Maritime Transportation Security Act provides that these issues are to be addressed through a rulemaking process. We look forward to working with BTS, Customs and TSA on these issues and such a process.

5. Contingency Planning

The Department of Homeland Security is now one year old, and is dealing with a very substantial number of issues. One of the issues that we hope will be high on the list of priorities for the coming year is the unpleasant topic of contingency planning, or how would trade be allowed to continue in the event of a terrorist attack on the industry? The issue first requires clear, agreed and practiced role definition within and among the various government agencies. But the implementation of any response scenario would also involve substantial activity by other governments, shippers, carriers, brokers, terminal operators, and others. Having some kind of dialogue and road map of expectations and requirements would be very helpful to the private sector. The World Shipping Council’s members are fully prepared to support and participate in any such endeavors.

6. Conclusion

Enhancing the security of America’s commerce has, in many respects, brought carriers, shippers, intermediaries and government closer together in addressing a common threat and dilemma. Simply hoping you are not the victim cannot be the approach, because a successful terrorist attack would make us all victims. It would affect every supply chain, every carrier, every port, and every nation’s trade and economy.

While trade and commerce, like many aspects of our society, remain vulnerable to premeditated criminal, terrorist activity, significant progress that has been made in the last year on enhancing the protection of international trade from the risk of terrorist attack. 2004 will certainly continue that progress, and while my remarks make it clear that these are not easy issues, the industry fully understands and supports working as closely as possible with the government to make commerce more secure in a way that is sustainable and does not unduly impede trade.