



WORLD SHIPPING COUNCIL
PARTNERS IN AMERICA'S TRADE

Remarks of
Christopher Koch

President & CEO of the
World Shipping Council

Before the

**Panama Canal Authority's
Conference on Maritime Security**

December 1, 2003

I. Introduction

During this year, the liner shipping industry and government policymakers have been addressing a host of important environmental, regulatory, and security issues. In this context, it is important to note the growing recognition among governments around the world about how important shipping is to our societies and our economies, to global trade, and to economic development. Sometimes that realization is heightened by disturbances to transportation, like the U.S. West Coast labor problems of a year ago. Sometimes governments' demonstrate that realization by enacting policy initiatives designed to support and maintain a maritime industry through new tax and promotional regimes. Sometimes one can sense this growing realization as reviews of liner shipping regulatory policy become more fact-based and rational, such as the recently contracted European Commission study on liner shipping which demonstrates that carrier agreements are not unregulated, harmful, price setting "cartels", but trade stabilizing organizations operating in a volatile, capital-intensive industry.¹ And, sometimes that

¹ See the World Shipping Council's website for a discussion of this recent report at www.worldshipping.org.

recognition is through the cooperative partnership that the industry continuously works to build with government to enhance the security of maritime commerce from the threat of terrorism.

Today, at the kind invitation of the Panama Canal Authority and its Administrator, Senor Alberto Aleman Zubieta, I would like to briefly discuss the issue of how much progress has been made on enhancing the security of maritime commerce and what some of the continuing challenges will be. While my remarks will discuss the various security measures being implemented by the United States government, it is essential to recognize that enhanced security of this international business requires international cooperation, and international consistency when possible. Nowhere is the need for effective cooperation more apparent than between Panama and the U.S., as roughly 60% of the 13,000 vessels transiting the canal each year call at U.S. ports.

We face a complex and multi-faceted challenge. But, if nothing else, the past two years' post-September 11 activities demonstrate that industry and government need to work closely together. There are no good alternatives to open, constructive dialogue and the joint development of effective responses to shared challenges.

To date there has been noteworthy progress, including the development of the International Ship and Port Facility Security Code (ISPS Code), the 24-hour advance cargo manifest filing requirements, the Container Security Initiative agreements, and the Customs' Trade Partnership Against Terrorism (C-TPAT) program. But even these programs are only beginning efforts that will continue to evolve, not completed projects.

Panama owns and operates arguably the most valuable maritime transportation asset in the world – the Panama Canal, and its flag registry is the largest in the world. It is taking a leadership role in the ISPS Code's implementation. It is therefore very appropriate that we are here in Panama at this conference to take stock of where we are and to plan for what more will need to be done. It is also appropriate as we gather at the center of the Western Hemisphere to examine how these evolving security rules will affect trade and commerce with Latin America.

In my remarks this morning, I would like to address several different components of the overall maritime security objective, namely enhanced ship security, facility security, personnel security, and cargo security.

II. Ships

We are seven months away to the day from the effective date of the International Ship and Port Facility Security (ISPS) Code and amendments to the International Convention for the Safety of Life at Sea (SOLAS), requiring vessel operators to develop and implement compliant vessel security plans. Compliance will require a significant effort, and this conference will spend considerable time addressing the requirements of the new code, so I will not try to address all of its components. But it is important to

recognize first, that the Code applies to approximately 50,000 vessels and thousands of port facilities globally, and second, that the Code is more than a set of procedural requirements and paper practices. It requires vessel operators not only to develop and implement the required measures, but also to have adequate resources available and trained to do the job.

Vessels that are not compliant by the July 1 effective date will, at best, face serious delays at the world's ports, and the U.S. Coast Guard has stated its intention to deny vessels without certificates entry to U.S. ports.

While all vessel registries, flag states and port states should be preparing diligently for this July deadline, I would like to address several issues that have arisen regarding the approach that the U.S. Coast Guard will be using for vessels calling at U.S. ports.

The first issue is the approval of vessel security plans. The Maritime Transportation Security Act (MTSA), passed by the U.S. Congress and requiring all vessels calling at U.S. ports to have vessel security plans, is being effectively implemented by the U.S. Coast Guard in a way that is entirely consistent with the new international rules and obligations successfully negotiated at the IMO. The Coast Guard deserves considerable credit for simultaneously and successfully partnering with domestic and international industry stakeholders, the IMO and other governments, other federal agencies and the U.S. Congress to accomplish this. The Coast Guard's approach to the implementation of the ISPS Code and SOLAS amendments, not only faithfully implements this new regime that the Coast Guard played a key role in creating, but it enhances maritime security through the use of a consistent, uniform international approach for our industry, which operates within the jurisdictions of all the maritime trading nations of the world. The Coast Guard regulations also clearly preempt individual U.S. states from establishing their own vessel security regulations, thus ensuring that the United States speaks with a single voice on these issues.

We believe that the Coast Guard's efforts in this regard can serve as a model for future American regulatory endeavors because its approach sought and achieves consistency and predictability amongst and between domestic and international requirements.

Flag states have the responsibility to ensure that vessels under their registry are compliant with the new requirements. The Coast Guard has clearly, consistently and repeatedly stated that the U.S. regulations neither invite nor require foreign flag vessels to submit their vessel security plans to the Coast Guard for approval. Advice to the contrary should not be followed. The Coast Guard is the agency that administers these laws in the U.S; it has clearly stated its position logically and forcefully in the regulations; it has clearly explained and defended the legal judgment behind its position; and, it has clearly and repeatedly stated that it will not accept foreign-flag vessel plans.

Although the House of Representatives has passed a bill that, if enacted into law would countermand this approach and require foreign flag vessels to submit their vessel security plans to the Coast Guard for approval, there is no comparable provision in the Senate version of the legislation, and such legislation is opposed by the Coast Guard and the Administration. And for good reason. Such an approach would be inconsistent with the international approach just recently and successfully concluded with the U.S. government's support at the IMO. It would establish the unfortunate precedent that every nation's vessel security plans would be subject to review and approval by every port state government where the vessel calls. Moreover, it would overwhelm the U.S. Coast Guard with plans that other governments are already responsible for approving under the ISPS Code. And, the Coast Guard has very clearly stated that it will use its port state enforcement authority to ensure that IMO compliant vessel security plans are in place.

Second, flag states and vessel operators cannot avoid their responsibilities under the Code, and the Coast Guard has made it abundantly clear that it will use its *port state* authority to inspect incoming vessels to ensure that foreign flag vessels seeking entry to the United States have approved plans by July 1, 2004 and have implemented adequate security standards in accordance with the ISPS Code and SOLAS amendments. The Coast Guard's port state control measures will also include tracking the performance of all owners, operators, flag state administrations, recognized security organizations (RSOs), charterers and port facilities. The Coast Guard intends to consider a vessel or port facility's history of compliance or lack thereof as important factors in the port state control equation. Non-compliance with the IMO requirements will subject a vessel to an array of control and compliance measures, from delay for a port state control boarding to denial of entry into port.

The collaborative development and implementation of these new vessel security rules by the appropriate combination of flag state and port state enforcement are not only an effective way to enhance maritime security on a global basis, but also to support three other important objectives. First, it demonstrates the U.S. government's commitment to and preference for developing international solutions to these challenges. Second, each successful international action builds effective momentum for the IMO to address other maritime challenges more effectively, such as vessel engine air emissions through Annex VI as it is ratified and becomes effective, such as the creation of a new IMO convention in February of next year to address ships' ballast water treatment and to prevent the unintentional transport of aquatic invasive species, and such as the IMO's possible development of a long-range vessel tracking system and regime. And third, this new regime illustrates how the international maritime community and governments can come together to establish and implement a uniform and internationally accepted enhancement of security.

III. Port Facilities

Each contracting government to SOLAS and the ISPS Code has the right and obligation to ensure that its port facilities are in compliance with the international

commitments laid down in those mandatory instruments. Contracting governments are required to make sure that security assessments are undertaken for their port facilities, and that security plans are developed that address identified vulnerabilities and meet the requirements of the Code.

One set of issues that will require better answers than are available today is – what are the consequences for a vessel with a compliant security plan when it arrives at a compliant port facility, if it has previously called at a port facility that is not in compliance during its voyage? This is not a theoretical question. It is likely that not all port facilities around the world will be compliant by July 1. Vessel operators need to know in advance whether and to what extent delays and added operating procedures and costs can be expected, so that they can plan accordingly. This is especially important for vessels that operate on fixed schedules, such as liner and cruise ships.

Another issue that has attracted attention internationally is the provision in the MTSA that requires the Secretary of Homeland Security to undertake foreign port assessments. This particular MTSA provision has yet to be implemented, but the Coast Guard's MTSA regulations state that the Coast Guard will be responsible for this function.

The U.S. Coast Guard has won the respect of the international community because of the integrity, sensitivity and professionalism that continues to characterize the service, and how it executes the obligations and rights as a port state to verify calling foreign vessels' compliance with international and domestic requirements. Foreign port assessments will require the same skills and professionalism.

They will also require diplomatic finesse and tact. One administration's request to be allowed to evaluate another administration's port security assessments and plans could be perceived as an expression of a lack of trust in the integrity and commitment of the host nation to abide by its international commitments -- *unless* the requesting administration makes such requests appropriately, conducts the evaluation with the full cooperation and involvement of the host nation, and in accordance with clear, accepted and verifiable criteria, and, shares the results and conclusions of the evaluation with the host nation.

Requests to evaluate foreign port facilities should also recognize the principle of reciprocity, i.e. a government that requests the ability to evaluate another nation's port facilities should do so in a way that it itself would find acceptable, non-intrusive and non-degrading if the host nation were to reciprocate by wanting to evaluate the requesting nation's port facilities.

We are confident that the Coast Guard would evaluate other nations' port facilities in such a considerate and transparent way. Mindful, however, of the particular interest devoted to this issue during the IMO negotiations and afterwards, we have encouraged the Coast Guard to develop a prudent and transparent framework for its foreign port assessments that can be shared, beforehand, with other nations' maritime

administrations, and which confirms the Coast Guard's intention to base such assessments on the criteria, standards and principles laid down in the relevant internationally agreed instruments, i.e. SOLAS and the ISPS Code.

IV. People

Within the United States, the Department of Homeland Security is developing a Transport Worker Identification Card for all domestic transport workers in each transportation mode, which will require government background checks and biometric identifiers. It is unclear when this system will become operational, but several pilot projects are underway, and it is possible that a system could become operational before the end of 2004.

Regarding seafarers, the United States has for many years had its own rules governing their entry into the country. After September 11 and in light of a number of reported cases of seafarers jumping ship and not returning to their vessels, and of the need to ensure that vessels do not become a pathway for terrorists to enter the country, the U.S. government has undertaken a number of changes to the rules affecting seafarers.

First, while no official decision has been announced, the U.S. government, effective last August, terminated its use of crew list visas, and now requires each seafarer to obtain an individual visa from a U.S. embassy or consulate. Because of both the general requirement that visa applicants be interviewed and backlogs in processing visas at U.S. embassies and consulates – particularly in seafarer producing countries, it is probable that seafarers may find that they cannot get a visa in time to sail. This can result in vessels arriving in U.S. ports with crew members aboard who do not have valid individual seafarer visas. In such cases, they will be unable to obtain shore privileges, and the vessel operator may incur additional costs of guards at the gangway. It may also result in difficulties for ship operators in scheduling signing off/signing on seafarers in U.S. ports.

Second, today information on all crew members is transmitted electronically to the Coast Guard 96 hours in advance of a vessel's arrival in a U.S. port, and upon arrival to Customs and Border Protection (CBP). Effective early next year, crew member information will also be required to be submitted electronically 96 hours in advance of arrival to CBP via its Advance Passenger Information System (APIS). The crew member information is used to screen these individuals through government information systems. Both agencies and the industry agree that there should be a "single window" for the advance electronic filing of such information that can be shared among government agencies. Yet both agencies continue to develop separate procedures and information systems, and the "single window" remains elusive. We have been working with the government and urging it to establish a single mechanism to file this information, and we will continue to advocate that this be done in 2004.

Third, in January of 2004 the U.S. will begin implementing “the United States Visitor and Immigrant Status Indicator Technology” -- commonly known as the US-VISIT program. The statutory deadlines are tight, and the information systems issues involved are very challenging, so it has come as no surprise that DHS is falling behind in implementing the program. The Department has therefore chosen to roll the program out in increments. This means that US-VISIT’s application to foreign seafarers seeking shore privileges, signing off, signing on, and transiting from one vessel to another in the United States will be fairly limited at first. Foreign seafarers will, however, have to comply with the program from January 5, 2004, when flying into and departing the United States by plane.

Fourth and finally, there is still a question about what role, if any, the new proposed International Labor Organization (ILO) seafarer credential may have in the United States. Although the U.S. government participated in the negotiations at the ILO that developed the new proposed seafarer credential, it was unable to clearly define what its objectives were in these negotiations, and cannot today articulate what purpose would be served by the new document, nor whether the ILO agreement will be sent to the Senate for ratification.

Seafarers still will need a passport and an individual visa with biometric identifiers that are not compatible with the proposed new ILO document’s, and the VISIT program is the system that -- also using biometric identifiers that are incompatible with the proposed ILO document -- will record entry and exit from the country. As a result, it appears that the ILO document would serve no role as a travel document in the U.S..

Some non-DHS government officials have alluded to the possibility that the card might be used to expedite seafarers individual visas², but there has been no action on this and no decision from DHS. The industry and other nations are obviously interested if there is a reason to implement this new credentialing agreement, and none has yet been articulated for the U.S. trades. We hope that DHS will address this issue in the near future.

As noted above, the industry recognizes the need for effective security measures and supports the government’s efforts to achieve that goal. But we do hope that, in 2004, the uncoordinated and duplicative processes governing seafarers arriving in the United States can be remedied, and that policy makers will recognize that the totality of all these various measures can cause significant difficulties and constraints for honest seafarers, who are in many respects a first line of defense in the maritime security effort.

V. Cargo Security

For ocean common carriers and many governments and shippers, cargo and container security has been a priority issue. In the United States liner trades, we have

² The World Shipping Council has submitted to the government detailed comments with some possible suggestions in this regard. See the Council’s website at http://www.worldshipping.org/iss_5.html for the most recent submission to the U.S. Department of State (September 4, 2003).

seen the implementation of the requirement to submit advance cargo manifest information to the government for security screening 24 hours before vessel loading in a foreign port, the development of Customs' Trade Partnership Against Terrorism (C-TPAT) initiatives, and the negotiation and implementation of Container Security Initiative (CSI) agreements between the U.S. government and its trading partners. Each of these is an important component of the effort to enhance security.

We have also seen the U.S and other governments try to get the World Customs Organization (WCO) to develop effective, mandatory uniform international container security standards, like the U.S. Coast Guard and the IMO did for ships and port facilities. Unfortunately, no Latin American Customs administrations have participated in the proceedings of the WCO's Task Force on Security and Trade Facilitation. The Council and U.S. Customs officials have worked diligently in support of this objective; however, it appears that the WCO is either unwilling or incapable, or both, of addressing container security in a meaningful and comprehensive way. It may yet produce guidelines or "best practices" for these issues, but this would seem to fall far short of an international instrument comparable to the ISPS Code. There are too many governments' customs officials at the WCO that either do not see cargo security as within their responsibility, or do not see it as an issue requiring meaningful WCO action.

What this means is that, without an effective international body addressing these issues, further U.S. cargo security measures will be undertaken either on a unilateral basis or pursuant to bilateral CSI agreements. In this regard, we welcome the announcement last month that the European Commission and U.S. government have agreed to intensify and broaden their Customs co-operation to improve the security of sea-containers and other shipments that are imported into, transhipped through or transiting the European Community and the United States. But it is also important that in the effort to address the largest volume trade lanes, that Latin America trades not be overlooked or disadvantaged. Accordingly, we encourage Latin American governments to, not only make sure that their vessels and port facilities are ISPS Code compliant by July 1, but that they carefully consider the steps involved and potential value in entering into CSI agreements.

As there is considerable regulatory activity in the area of containerized cargo security, let me briefly touch on developments in each of the following areas: secure container loading, cargo documentation and screening, and in-transit security.

A. Secure Container Loading

Secure container loading is the starting point, and arguably the single, most important point, in the container security process. It is also the most difficult to address because it involves millions of containers being loaded at tens of thousands of different locations in every country in the world. An ocean carrier is like the postman; it receives a sealed container for transportation, and has no first hand knowledge of what has been loaded inside. Unless the carrier is aware of information that arouses its suspicion about a particular container, it has little choice but to trust what shipping documents state is in the container and that the loading process was secure.

The Customs Trade Partnership Against Terrorism (C-TPAT) program is one way to try to effect improvements in this regard, but this is a substantial challenge. We expect that the Bureau of Customs and Border Protection (CBP or Customs) will continue to try to expand the voluntary C-TPAT program into an initiative that includes manufactures and suppliers outside the United States. It is also noticeable that the focus of C-TPAT has been on the largest volume trades and on the inclusion of European and Asian manufacturers. This could have implications for the ability of Latin American exports to the United States to qualify for the "low risk" status and any associated benefits under the C-TPAT program. We expect other governments and shippers themselves will continue to take measures to tighten supply chain security. But it is a tall order, and will also require continued developments in the areas of cargo documentation and screening.

B. Cargo Documentation

Cargo documentation and screening has been one of the most active areas of change, and we expect 2004 will see this continue. We began 2003 with the implementation in U.S. trades of the requirement to file cargo manifests with Customs 24-hours before vessel loading. This change, while substantial, has been implemented relatively smoothly and has involved a very open and cooperative relationship between the industry and government. We understand its importance and its relevance to the security strategy being deployed. But some further changes are apparent, and some -- that are not presently apparent -- are inevitable. I will try to briefly list some of these that will affect U.S. international commerce:

1. Trade Act Regulations: U.S. Import Cargo

At the end of this week, CBP will publish new regulations implementing requirements of the Trade Act of 2003 and addressing cargo documentation requirements for all transport modes. For ocean shipping, one of the more significant issues will be how the final Customs regulations differ from the proposed regulations' efforts to require the "shipper" box on a transportation bill of lading to state the name of an importer's actual supplier. The issue is complex. Time does not permit a full discussion of that issue here today, but the Council's detailed August 22 comments to CBP on this topic can be found on our website.

2. Trade Act Regulations: U.S. Export Cargo

We understand that the new regulations will require U.S. exporters to file an electronic Shipper's Export Declaration (SED) for export vessel cargo directly to the government via the Automated Export System (AES) no later than 24 hours prior to vessel departure. The carrier may not load export cargo without first receiving from the U.S. exporter either the electronic SED filing confirmation number or an appropriate exemption statement. There are expected to be several exemptions from the advance SED export cargo filing requirement depending on the value of the shipment, the size and nature of the U.S. exporter, and possibly also the types of cargo.

The Trade Act export information requirements can only take effect once another rulemaking from another government agency (U.S. Census), requiring the electronic submission of SEDs, has been proposed and taken effect. Therefore, these export cargo requirements will likely take effect in the fall of 2004.

3. Food Import Regulations:

The U.S. Congress recently passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (“Bioterrorism Act”), which requires food facility registration and prior notification of certain imported food be provided to the U.S. Food and Drug Administration (FDA) before its arrival in the United States. While these regulations become effective on December 12, FDA and CBP recognize that this new system is untested and replete with potential problems, and therefore have indicated their intent to not enforce penalties or delay cargo shipments in the first several months of the rules’ implementation.

Because the United States imports approximately \$50 billion worth of food products, and because these rules are so extensive and new, considerable effort and adaptation by food shippers, brokers and carriers will be needed.

First, these regulations require every facility in the world that produces or holds FDA-regulated food products shipped to the United States to register with the FDA and have a U.S. agent. Second, they require every FDA regulated food shipment to file detailed information about the product prior to its arrival in the United States, and they identify carriers as the parties through whom the government will stop cargo that is not compliant with the new rules.

While some issues remain unclear³, some things about these rules appear likely:

- Documentation of FDA regulated food shipments that travel to or through the U.S. will become much more complicated, and failure to comply will mean that, after the initial transition phase is over in early 2004, the imported food will not be released from the U.S. port of arrival.
- Foreign food shipments to Canada and Mexico will encounter much simpler documentation requirements if they are unloaded at a Canadian or Mexican port than if they travel through a U.S. port.
- Foreign food shipments to the U.S. are likely to encounter less chance of documentation problems if they are unloaded at a U.S. port than if they are brought to the U.S. via Canadian or Mexican ports.

³ For more information on these new food import regulations, visit the FDA’s website at: www.fda.gov/oc/bioterrorism/bioact.html

FDA has invited another round of public comments on these rules to be submitted by December 24. The Council and many others will be filing comments.

C. Cargo Screening and Inspection

For U.S. containerized shipping, CBP, together with a growing number of other government's customs authorities, are screening information about cargo shipments more closely. The documentation of 100 percent of all imported containerized cargo shipments is screened by CBP for security purposes before vessel loading. Any shipment that does not pass the applicable risk assessment criteria is then subject to inspection.

Governments and ports are deploying more X-ray, gamma ray, and radiation detection inspection equipment. Since September 11, CBP has more than doubled the number of containers that it physically inspects, and that number is likely to continue to rise as shipment screening capabilities become more robust, as the availability of non-intrusive container inspection equipment increases, and as initiatives such as C-TPAT become more prescriptive. The CSI initiative is also developing the necessary, reciprocal government operating arrangements that can allow shipments to be inspected at the port of loading, and not just the port of discharge.

I would like to briefly mention two aspects of these container inspection and screening developments. One involves the implications for marine terminals, and the other involves the improvement of the risk assessment screening.

Marine terminals serving U.S. trades need to consider the importance of working with U.S. and other government authorities to undertake effective cargo security planning. For example, a port facility handling transshipment cargo that is ISPS Code compliant and at a CSI port may be more attractive for shippers and carriers to deal with than one that is not – because ship schedules and cargo flows are likely to be more predictable and efficient than if the port facility is not compliant or security questions about cargo cannot be addressed at origin. Similarly, terminal facilities would be better prepared to keep trade flowing through their port after a terrorist incident if they are ISPS Code compliant and in CSI ports. There are indeed challenges involved, such as planning for how and where the increase in container inspections can be accommodated at ports without unduly disrupting operations, and such as how smaller ports can undertake the steps necessary to become CSI ports. But, if a port believes that cargo security challenges can simply be left to carriers and the receiving ports' government to handle, one should not be surprised if trade through that port may encounter increasing difficulties under the evolving rules. We note that a number of U.S. port facilities are going significantly beyond minimum requirements and are, for example, deploying radiation detection technology that is used on all containers entering and leaving the facility.

The second issue in this regard is the improvement of shipment risk assessment screening. As discussed earlier, carriers' cargo manifests have been the best available

advance cargo information for the government to use for risk assessment pre-screening of cargo. The Council and its Members have strongly supported Customs' implementation of the 24-hour rule to get this data earlier, and this system has clearly improved trade documentation practices and the information the government receives.

As U.S. Secretary of Homeland Security Ridge has stated: "Advance information is a cornerstone in our efforts to secure our nation's borders and ensure the flow of trade." With advance information playing such an important role, the quality of that advance information will certainly receive closer scrutiny. The present information system for U.S. import ocean carriage has known limitations.

First of all, the bill of lading data that is used is only the data the carrier needs for its transportation responsibilities, and much of it is not within the direct knowledge of the carrier, but is second hand information. To improve the quality of that data one must recognize that shippers often will not fully disclose commercial data to their carrier. Occasionally, this may not be for legitimate reasons, but it may be for entirely legitimate, commercial reasons. The data that the government needs that is within the knowledge of the shipper should be derived from and filed by the shipper.

Second, there are data gaps in the present system. For example, bills of lading may, but may not, capture information about the origin or prior handling of the shipment. A port-to-port bill of lading will not reveal the history of the shipment prior to the originating port. The carrier may not possess this information, and relying only on its bill of lading provides an incomplete picture of the risk profile of a shipment. These kinds of issues should cause the government to undertake a security "gap analysis" to assess what data the government needs, from whom, when in order to improve its security-screening capability.

One should not underestimate the fact that this is a difficult and complex area, but there is also an excellent opportunity to address these issues in the coming year. CBP is in the process of developing and rolling out in stages its new Automated Commercial Environment system (ACE). Now is the time for that system to be designed to incorporate new cargo screening security requirements and to determine what new data is needed, from whom, when -- as the program is designed.

D. In-Transit Container Security

While the secure initial loading of a container and the effective application of sound risk assessment to shipments are essential to the security of international commerce, it also true that the security of a container while it is in transit is very important. It is the third component of the cargo security strategy of addressing the secure stuffing of the container, the effective screening and risk assessment of the container, and the secure transit of the container.

Recognizing that fact, the World Shipping Council's Security Advisory Committee, together with the International Mass Retail Association and the National Industrial Transportation League, developed and submitted to the U.S. government and the World Customs Organization a White Paper outlining a set of recommendations on the issue.⁴ It recommends a set of regulatory requirements applicable to all containerized shipments, and offers some initial observations on the questions of how technology might be considered in addressing the issue of detecting in-transit tampering with shipments.

The issues involved are not simple as they touch on numerous jurisdictions, numerous commercial parties and their operating practices, and government information systems and responsibilities.

When the multitude of potential, future technology products are added to the consideration of this issue, these issues become even more complicated.

The path forward requires clarity in deciding what the security requirements should be, and the essential need to address -- not just what a technology proponent says its device can do -- but a clear and candid assessment of the operational and information system implications, roles and responsibilities of a technology. The debate and analysis in this regard has been poor at best. Why? Because it is difficult.

It is much easier for a technology vendor to say we need a "smart" container and my device will make it "smarter", than it is to clearly articulate and establish:

- What is the security requirement we are trying to establish and address, and does the government agree?
- What are the operational implications and demands for the device to meet those requirements when it is deployed in the international commercial environment?
- What information is generated by the device, who receives it, whose information system is responsible for it, who has access to it, and who is responsible for acting on it?
- Does it work? For example, does it create a significant number of false positive alerts?
- If it is to be operated by the private sector rather than the government, where does the technology vendor earn its revenues in the process?
- And, if it is to be operated by the private sector rather than the government, is the requirement capable of being met through a competitive market of equivalent products?

In the United States, there is a program in the Transportation Security Administration – Operation Safe Commerce – that may be addressing some aspects of

⁴ The White Paper, entitled "In-Transit Container Security Enhancement", dated September 9, 2003, can be found on the Council's website.

these issues; however, because the industry has little visibility into these efforts, we are unable to provide an assessment of that program at this point.

There is also an evolving effort led by CBP through the C-TPAT program to develop a C-TPAT “smart and secure container”, which will need to address these issues. CBP, which plans to begin testing this concept with a limited number of C-TPAT importers beginning in January of 2004, has expressed the objective of linking expedited processing and cargo release to multiple components of a secure supply chain. Specifically, this pilot program appears to envision: 1) a foreign vendor or manufacturer that meets C-TPAT security standards at the point of loading (“stuffing”), or a C-TPAT importer who has assured that its foreign vendors meet C-TPAT security standards at the point of stuffing; 2) a C-TPAT “smart and secure container” (meaning one that uses a high security manual seal, a secure application of the seal in a location other than the door handle, and an intrusion sensor); 3) shipment through a foreign port that participates in the CSI program; 4) carriage by a C-TPAT carrier; and 5) delivery to a C-TPAT importer.

CBP has stated that it will be the party reading the sensor in this pilot program. Should this pilot prove the sensor to be an effective and workable device, a key question of interest to every terminal operator, shipper and carrier, if the system is to be made applicable to trade generally, will be whether CBP plans to continue in the role of sensor reader, or whether terminal facilities around the world will be expected to implement this for C-TPAT shippers in U.S. commerce. The former approach would substantially reduce the number of issues and obstacles that would have to be considered. While there are numerous questions about how this initiative will proceed, Customs has worked closely with the industry and other governments in the past, and we expect that they will work to build on that partnership going forward.

VI. Conclusion

Each of the initiatives discussed above, involving ships, port facilities, people, cargo security, cargo screening, inspection, and risk assessment capabilities is an important part of a multi-layered effort to enhance the security of international commerce. It is a complex and multi-faceted security infrastructure that is being built, but we now live in a world where it must be built, and all sectors of industry and all trading nations must work together to help create it.

We should also recognize that the security infrastructure we are trying to build to prevent terrorists from using or attacking international maritime trade needs to be built to be robust enough to function as the security infrastructure that will be used to keep trade flowing in response to an incident.

It thus must not only be effective in design, but all the players’ roles and responsibilities should be clear. Ambiguity in the face of difficult questions is

understandable, but it neither advances effective security, nor helps government or industry understand what it needs to do to adapt to meet these evolving needs.

We are making substantial progress in enhancing the security of international trade. The system is certainly more secure now than it was two years ago. It will be even more secure next year. But, as I stated at the beginning of my remarks, the past two years' post-September 11 activities demonstrate that industry and government must work closely together. There are no good alternatives to open, constructive dialogue and the joint development of effective solutions to shared challenges.