Testimony of

Christopher Koch

President & CEO of the

World Shipping Council

Regarding

"The State of Maritime Security"

Before the

Senate Committee on Commerce, Science and Transportation

March 24, 2004

Introduction

Mr. Chairman, I would like to thank the Committee for the opportunity to comment on the state of maritime security enhancements. My name is Christopher Koch, and I am the President and CEO of the World Shipping Council (WSC). The Council is a non-profit association of thirty companies that operate forty-four international shipping lines. WSC's members include the full spectrum of vessel-operating ocean common carriers, offering containerized, roll-on/roll-off, car carrier, and other international cargo transportation services. WSC's members carry approximately ninety-three percent of the United States' imports and exports transported by the international ocean liner shipping industry.

International commerce is a huge and economically vital part of our economy, and liner shipping is an essential facilitator of that trade. In 2002, approximately 202,800 U.S. importers received goods from more than 178,200 foreign exporters via liner shipping. The combined value of U.S. exports and imports of goods moved by international waterborne trade in 2002 was approximately $728.4 billion. Close to $500 billion, or two-thirds of that, was containerized cargo carried on liner vessels. On average, roughly $1.4 billion worth of goods are moved through U.S. ports by the liner shipping industry each day.

The Council has strongly supported the various efforts of the government to enhance maritime security, and it will continue to do so. Whether it has been the Coast Guard's efforts as the lead agency for vessel and port security, or Customs and Border Protection's efforts as lead agency for cargo security, the Council has fully supported the government's strategies in both domestic regulation and in international fora.

Enhancing maritime security, while maintaining the efficient flow of commerce, is a very large, complex and multi-faceted task, and this Committee's oversight of that effort is very appropriate. In my remarks this morning, I would like to address several different components of the overall maritime security objective, including enhanced ship security, port facility security, personnel security, and cargo security.

I. Ship Security

The Maritime Transportation Security Act instructs the Coast Guard to establish regulations requiring all vessels calling at U.S. ports to have vessel security plans. With an upcoming July 1 effective date, all vessels arriving at U.S. ports will have to be fully compliant with the new International Ship and Port Facility Security (ISPS) Code and the amendments to the International Convention for the Safety of Life at Sea (SOLAS). The Coast Guard deserves considerable credit for simultaneously and successfully partnering with domestic and international industry stakeholders, the International Maritime Organization 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 international 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 an industry, which operates within the jurisdictions of all the maritime trading nations of the world.

Vessels that are not compliant with the Code by the July 1 effective date will be denied entry to U.S. ports. The Coast Guard regulations will ensure that every vessel has an approved security plan, designated and trained personnel responsible for defined security actions and communications, procedures for communicating with ports and other vessels, procedures for monitoring and controlling physical security and access to the vessel, and the installation of Automated Identification Systems transponders.

While a substantial amount of work is being done to be compliant by July 1st, our Member lines' representatives have identified no significant problems regarding lines' expectations that their vessels will be compliant by that time.

We would note that the new rules require most ships to have AIS transponders installed and operational by July 1,[1] but that Coast Guard receiving stations will not be operational by that time in a number of U.S. port regions, especially along the Atlantic and Gulf coasts. We believe that the Coast Guard should be given the resources to make a nationwide AIS system fully operational as soon as possible.

Finally, we note that while these vessel security plans will improve internal vessel security and preparedness as intended, they may be of little defense against an organized, external terrorist attack of a merchant vessel, such as the attacks on the *Limburg* or the *U.S.S. Cole*.

II. Port Security

The regulations established by the Coast Guard to implement the requirements of the Maritime Transportation Security Act and the ISPS Code also require port facilities to be compliant by July 1st. As with vessel security plans, compliance with these requirements may involve considerable effort, but, as with vessels, we are unaware of any U.S. container terminal that does 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' maritime authorities when they arrive after having called during their voyage 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.

[1] All vessels larger than 50,000 gross tons are required to comply by July 1,2004. Vessels less than 50,000gt but larger than 300 gt must comply not later than the first safety survey, but not later than December 31.

Similarly, it is currently unclear what consequences shippers should expect for their cargo that passes through noncompliant facilities. 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, we expect it is likely to undertake measures designed to impose pressure on such ports and governments to comply, 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. In short, while we fully recognize that the U.S. and other ISPS Code compliant nations are likely to take actions that will affect carriers and shippers that move cargo through a non-compliant foreign port facility, and that such actions are likely to be designed to ensure, inter alia, that all parties strongly support efforts by all port facilities to become compliant as soon as possible, it is unclear at present how these situations will be addressed.

III. Personnel Security

The Transportation Security Administration 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. This system will apply to shore-based, domestic maritime workers. It is unclear when this system will become operational, but several pilot projects are underway.

Regarding U.S. and foreign seafarers, the government has undertaken a number of changes.

First, it reviewed all U.S. seafarers and revoked the licenses of a number of persons who raised security questions.

Second, for foreign seafarers, effective last August, the use of crew list visas has been terminated. Each seafarer is required to obtain an individual visa from a U.S. embassy or consulate, and undergo a personal interview. If a seafarer does not have an individual visa, he will be unable to sign on or off the vessel in the U.S. or obtain shore privileges in the U.S., and the vessel operator may incur additional costs of posting guards at the vessel gangway.

Third, 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 is provided separately to Customs and Border Protection (CBP) and is screened 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. One of the positive manifestations of effective coordination within the new Department of Homeland Security is the recent agreement by the CBP and Coast Guard that the Coast Guard's electronic notice or arrival (e-NOA) system will soon be an acceptable "single window" system for this purpose and will be used by both agencies,

thus eliminating duplicative filing requirements. We would like to commend Undersecretary Hutchinson, the Coast Guard and Customs and Border Protection for their continued efforts in this regard.

IV. Cargo Security

One of the most complex challenges is the enhancement of cargo security, especially containerized cargo. The vast majority of liner cargo is containerized – that is, it is carried in sealed metal containers from point of origin to destination. These containers come in standard sizes (typically 20', 40', and 45' in length) and may include various specialized technologies, such as refrigeration units for chilled and frozen foods, or internal hanger systems for carrying garments. Over 20 million TEUs (twenty foot equivalents) of containerized cargo are imported or exported through U.S. ports per year. Containers serve, in essence, as a packing crate and in-transit warehouse for virtually every type of general cargo moving in international commerce.

Physically inspecting every container is not practicable. Commerce would be severely disrupted.

A. Cargo Screening and the Automated Targeting System

As a result, Customs has developed and implemented a strategy to enhance the security of containerized cargo by:

- Requiring carriers to provide the agency with advance cargo manifest information for *every container* imported into the U.S. (or stowed aboard a vessel that calls at a U.S. port even though the cargo may be destined for a foreign country), 24 hours before vessel loading in a foreign port,
- Analyzing such information via the agency's Automated Targeting System (ATS),
- Inspecting any container about which ATS raised significant questions, and
- Developing close cooperative working relationships with the governments of our trading partners through the Container Security Initiative.

The ATS is thus a central feature in determining which containers get inspected and in the working relationships that Customs is establishing with other federal agencies and with other trading nations' Customs administrations.

It is noteworthy that with international liner shipping, unlike the other freight transportation modes[2], the government strategy is to perform cargo security screening before the cargo is even 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 have arisen.

[2] Cargo carried on passenger aircraft is also subject to screening/inspection prior to aircraft loading.

The Rule's importance is obvious to the security strategy described, and ocean carriers have supported Customs' strategic initiative and the Rule.

Today ATS is populated with carriers' cargo manifest or bill of lading data, and it utilizes other government data. A significant pending question is whether the current 14 cargo manifest data elements are sufficient for the security task at hand. Earlier this year the complexities of this issue became obvious in the context of Customs' Trade Act cargo documentation regulations. Customs amended the cargo manifest regulations' regarding 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". This particular approach to obtaining such information presented serious problems.[3]

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 remain 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:

> "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

[3] For a complete explanation of all the issues created by this proposal, the Council's petition that was submitted to Customs on February 2 can be found on the Council's website. www.worldshipping.org.

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 importers 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 difficult but 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.

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 apparent that carriers should not 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, which indicates carriers should not be the parties filing this kind of 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 filing requirements are becoming more prevalent with Customs administrations 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.

B. 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. It then has the ability to inspect, via physical de-vanning of a container or use of Non-Intrusive Inspection technology (gamma ray or x-ray), every container that raises a security question. As Customs 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 are likely to continue to increase. We believe that a numerical objective, however, 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 CSI foreign ports of loading we cannot tell at this time.

Finally regarding container inspections, Customs has stated that its goal is to establish radiation-screening portals that will perform radiation screening on 100% of all containers 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. We also note that some foreign ports are undertaking similar measures to protect international commerce and that the Port of Rotterdam is implementing a similar radiation screening system.

C. Container Security Initiative

I began my testimony by 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, however, 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, and the Council hopes that all participating governments will implement these CSI agreements effectively and cooperatively. Of the 38 CSI ports, 18 are currently operational.

CBP deserves a lot of credit for where it has taken this initiative, and while we recognize that many details of CSI have not been spelled out, we would urge the Committee to consider that the program is still in its developmental stage. Ocean carriers are fully supportive of these initiatives. In the event governments need to respond to a terrorist event in this industry, it seems likely that trade would be irreparably harmed if CSI agreements are not operational and well implemented

D. 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.

The objective of this exercise is generally stated to be 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. Electronic seals (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.

Consideration of e-seals usually involves 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 were 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 developing standards for RFID e-seals and tags, and has submitted 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 it be RFID, wireless or satellite 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?
- How does the technology 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 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.

Finally, there is the issue of how "sensors" might be applied to containers. Clarity will be needed on what should be sensed, and where. For example, 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, which might be disabled by a terrorist loading the container?

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 are considering whether satellite and/or wireless technologies may be 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 will have significant cost and operational implications for customs administrations, shippers, carriers, and terminal operators around the world.

In this regard, 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 BTS Directorate has also announced that it will soon be establishing a new consultative process with the industry to help consider and address the issues involved. It is not entirely clear at this time how the ongoing "smart" container analysis within Customs and within Operation Safe Commerce will be integrated into this process, but it presumably will be. We look forward to working with BTS, Customs and TSA on these issues and such a process.

E. Customs Trade Partnership Against Terrorism (C-TPAT)

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 and sealed 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 with all the necessary cargo documentation regarding the shipper, the consignee, and the cargo, but it 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, and that it will continue its efforts to validate compliance.

F. Export Cargo Regulation

Later this year, the Census Bureau is expected to issue new regulations requiring 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. Once those regulations are in place, a 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.

G. Imported Food Security

The United States imports approximately $50 billion worth of food products per year. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 requires food facility registration and requires that prior notification of certain imported food be provided to the U.S. Food and Drug Administration (FDA) before its arrival in the United States. The implementing regulations require facilities throughout the world that produce or hold 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.

This is a complicated and extensive new regulatory system that is being developed, and we would like to commend Customs and Border Protection for their extensive efforts to assist FDA in making these new regulations as workable as possible.

V. 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 Department 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 U.S. government agencies. Second, it requires clear understandings and practiced scenarios with the governments of our trading partners who presumably will have just as significant an interest and need to address the continuation of commerce as the U.S. government. Third, the implementation of any response scenario would also

involve substantial activity by the private sector – importers, exporters, 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.

VI. Conclusion

Mr. Chairman, the above is a brief description of the major security enhancement initiatives as they affect international liner shipping. While liner shipping is the largest component of our maritime commerce, it is important to recognize that there are many other maritime sectors that are not addressed herein, including the passenger cruise industry, the bulk and tanker shipping sector, the inland waterway industry, break-bulk cargo, and small vessels calling at small facilities. Each sector has its separate and distinct security challenges.

In the liner shipping sector, 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 has been made in the last year to enhance the protection of international trade from the risk of terrorist attack. But this is a work in progress that must continue. 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 robust enough to function as the security infrastructure that will be used to keep trade flowing in response to a transportation security incident.

The security infrastructure thus must not only be effective in design, but all the players' roles and responsibilities in that system should be clear. Ambiguity in the face of difficult questions is quite 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. We fully recognize that it is a difficult challenge, and that industry and government must work closely together to meet the challenge. There are no good alternatives to open, constructive dialogue and the joint development of effective solutions to shared challenges. We would like to state for the record that the agencies responsible for maritime security, particularly the Coast Guard and Customs and Border Protection, have consistently worked closely with the industry in these efforts. The international liner shipping 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.