WORLD SHIPPING COUNCIL
PARTNERS IN TRADE

Statement of

Christopher Koch

President & CEO
World Shipping Council

Before the

House Homeland Security Appropriations Subcommittee

Regarding

"Container, Cargo and Supply Chain Security – Challenges and Opportunities."

April 2, 2008

I. Introduction

Chairman Price and members of the Subcommittee, thank you for the invitation to testify before the Subcommittee today. My name is Christopher Koch. I am President and CEO of the World Shipping Council (WSC or the Council), a trade association that represents the international liner shipping industry. I also serve as the Chairman of the National Maritime Security Advisory Committee (NMSAC), a Federal Advisory Committee Act committee providing advice to the Coast Guard and the Department of Homeland Security (DHS) on maritime security issues, and as a member of the Commercial Operations Advisory Committee (COAC) that advises the Departments of the Treasury and Homeland Security on commercial and Customs matters.

Liner shipping is the sector of the maritime shipping industry that offers regular service based on fixed schedules and itineraries. The World Shipping Council's liner shipping member companies provide an extensive, network of services that connect American businesses and households to the rest of the world. WSC member lines carry roughly 93% of America's containerized international cargo.[1]

[1] A listing of the Council's member companies and additional information about the Council can be found at www.worldshipping.org .

Approximately 1,500 ocean-going liner vessels, mostly containerships, make more than 26,000 U.S. port calls each year. More than 50,000 container loads of imports and exports are handled at U.S. ports each day, providing American importers and exporters with efficient transportation services to and from roughly 175 countries. Today, U.S. commerce is served by more than 125 weekly container services, an increase of over 60% since 1999.

In addition to containerships, liner shipping offers services operated by roll-on/roll-off or "ro-ro" vessels that are especially designed to handle a wide variety of vehicles, including everything from passenger cars to construction equipment. In 2006, these ro-ro ships brought almost four million passenger vehicles and light trucks valued at $83.6 billion into the U.S. and transported nearly one million of these units valued at $18 billion to U.S. trading partners in other countries.

Liner shipping is the heart of a global transportation system that connects American companies and consumers with the world. More than 50 percent of the $1.8 trillion in U.S. ocean-borne commerce is transported via liner shipping companies.

The international liner shipping industry has been determined by DHS to be one of the elements of the nation's "critical infrastructure".

Liner shipping generates more than one million American jobs and $38 billion in annual wages. This combined with other industry expenditures in the U.S. results in an industry contribution to U.S. GDP that exceeds $100 billion per year.

II. Maritime Security

For the past six and a half years, the WSC and its member companies have strongly supported the various efforts of the U.S. Coast Guard and U.S. Customs and Border Protection (CBP) to enhance maritime and cargo security. The multi-faceted and risk-based strategies and programs of the government have been able to make substantial progress toward meeting this challenge, and they continue to evolve.

At the same time, the Coast Guard and CBP recognize the fact that the industry is transporting on average roughly 50,000 containers, holding roughly $1.8 billion worth of cargo owned by U.S. importers and exporters, each day through U.S. ports. Significant delays to this flow of legitimate commerce could have substantial adverse effects on the American economy.

The basic architecture of U.S. maritime security is well known and understandable. First, there is *vessel and port security*, overseen by the Coast Guard and guided in large measure by the International Ship and Port Facility Security Code. Second, there is *personnel security*, overseen by various DHS agencies and the State Department. Third, is *cargo security*, which with regard to containerized cargo, is addressed through CBP's advance cargo screening initiative, C-TPAT, and the Container Security Initiative – all of which are reinforced and made more effective by the increased deployment of container inspection technology at U.S. and foreign ports. While recognizing that the subject of this hearing is cargo and supply chain security, I would like to briefly touch on the other parts of the DHS strategy before discussing the cargo and supply chain security developments.

A. Vessel and Port Security

Every commercial vessel arriving at a U.S. port and every port facility needs to have an approved security plan overseen by the Coast Guard. Each arriving vessel must provide the Coast Guard with and an advance notice of arrival 96 hours prior to arriving at a U.S. port, including a list of all crew members aboard – each of whom must have a U.S. visa in order to get off the ship in a U.S. port.

The liner shipping industry's operations are consistent and repetitive – its vessel services and crews call at the same ports every week. So long as there is consistent and professional implementation of the security rules, which is usually a hallmark of the Coast Guard, liner shipping has found little problem in operating in the new vessel or port security environment.

We also appreciate the Coast Guard Commandant's admonition that the "concept of maritime security cannot be reduced to a single threat vector". There are numerous potential vectors for terrorists attack on the maritime environment that don't involve cargo containers. For example, merchant vessels are in fact defenseless against small boat attacks. We fully support the Coast Guard in its efforts to secure an enormous Maritime Domain against a variety of risks.

Long Range Information and Tracking (LRIT) of Vessels: In October, the Coast Guard published a Notice of Proposed Rulemaking (NPRM) on Long Range Information and Tracking (LRIT) in the Federal Register. The Council supports the LRIT program and the substantially enhanced visibility of vessels offshore that it will give to the Coast Guard and other governments. This new initiative is scheduled to become operational by January 1, 2009

Small Vessels: The attacks on the *U.S.S. Cole* and *M/V Lindbergh* demonstrated that large vessels can be the objects of terrorist attack from small boats. The U.S. Coast Guard Commandant, Admiral Allen, has on numerous occasions noted this and other small boat vulnerabilities and the difficulty in devising effective ways to address the threat without significantly inconveniencing recreational and small boat movements. The Council notes that DHS has recently undertaken some pilot efforts on the West Coast to test technologies that may contribute to addressing this issue, and while we recognize the difficulty of the challenge, we believe that such DHS efforts are focusing on a legitimate concern.

B. Personnel Security

The Council supports the Transportation Worker Identification Credential (TWIC) program, mandated by Congress and being established by the Coast Guard and the Transportation Security Administration (TSA) to credential workers requiring unescorted access to secure maritime facilities. The National Maritime Security Advisory Committee (NMSAC), with the advice and input of a wide range of U.S. maritime interests, has spent considerable effort to provide comments to the Coast Guard and the TSA on the development of the TWIC regime. The industry's primary concern is that the security enhancements envisioned in this new system not have undue impacts on those personnel who work in port terminals servicing vessels or on port operations.

III. Cargo and Supply Chain Security

The WSC supports the DHS strategy addressing containerized cargo security, and the way that CBP has worked to execute that strategy while minimizing inconveniences to commerce. Specifically, the Council supports:

1. CBP's risk assessment and screening of 100% of all cargo containers prior to their being loaded onto vessels destined for the U.S.,
2. the pending proposed rulemaking by CBP to improve the agency's cargo risk screening capability through the acquisition of more complete and accurate information about such shipments (the "10 plus 2" initiative),[2]
3. the pre-vessel loading inspection of 100% of those containers that CBP's cargo risk assessment system determines to present a substantial security risk or question; and
4. radiation scanning of all containers at U.S. ports, and non-intrusive inspection (NII) of all containers at U.S. ports that present any sort of question that was not addressed at the foreign port of loading.

A. Container Security Initiative (CSI)

The network of bilateral Customs-to-Customs agreements forming the "Container Security Initiative" (CSI) continues to grow. CBP states that there are 58 foreign ports participating with the U.S. in this initiative, covering 85% of U.S. containerized import trade. CSI is a keystone to the effective international implementation of the advanced screening and inspection of U.S. containerized cargo that presents security questions. It is only through these cooperative CSI Customs-to-Customs data sharing and container inspection cooperative efforts that overseas container inspection can occur.

Containerized commerce is a two-way street, and adequate documentation procedures for U.S. export commerce must also be addressed. More than five years after Congress passed the supply chain security amendments to the Trade Act, disagreement between the U.S. Departments of Homeland Security and Commerce has prevented regulations from being issued to implement Section 343(b) of that Act (19 U.S.C. 2071(b)), which calls for rules regarding the advance documentation of U.S. export waterborne commerce. We understand from CBP that this logjam has been resolved and that proposed regulations should be published soon.

B. Containerized Cargo Screening and Risk Assessment

CBP employs a multi-faceted containerized cargo risk assessment and screening system, so that it can identify those cargo shipments that warrant further review, rather than those that are low risk and should be allowed to be transported without delay.

C-TPAT: One element of that system is the Customs' Trade Partnership Against Terrorism (C-TPAT) pursuant to which various entities in the supply chain voluntarily

[2] The Council's comments to CBP on the "10 plus 2" Notice of Proposed Rulemaking can be found on the WSC website at www.worldshipping.org .

undertake security enhancing measures. CBP then validates participants' compliance, and compliant supply chains are accordingly afforded lower risk assessments.

24 Hour Rule: A central element of the cargo risk assessment system is CBP's receipt and analysis of pertinent advance information about cargo shipments before vessel loading. This program began soon after September 11th, under which carriers provide CBP with the advance shipment information they possess 24 hours before vessel loading in a foreign port for risk screening (the "24 Hour Rule"). The Council has fully supported this regulation and this strategy, which allows the CSI program to perform advance container risk assessment.

Better Security Screening Data: "10 plus 2" Initiative: While the 24 Hour Rule has been a logical and sound effort, CBP has determined that more effective advance cargo security screening will require more data than the information provided by carriers via the 24 Hour Rule.

Recognizing both this need for enhanced container security targeting and the existing limits of information provided in carriers' bills of lading, Congress in the SAFE Port Act required CBP to enhance the capability of its Automated Targeting System:

> "Section 203(b): Requirement. The Secretary, acting through the Commissioner, *shall require* the electronic transmission to the Department of *additional data elements for improved high-risk targeting*, *including appropriate elements of entry data* … to be provided as advanced information with respect to cargo destined for importation into the United States *prior to loading of such cargo on vessels at foreign ports*."

In early January, Customs and Border Protection (CBP) issued a proposed regulation that would require U.S. importers or cargo owners to file ten additional data elements[3] with CBP 24 hours prior to vessel loading, and to require ocean carriers to provide two additional sources of data -- vessel stowage plans prior to arrival in the U.S., as well copies of electronic container status messages. This initiative, commonly referred to as "10 plus 2", is an effort that CBP has been discussing with the trade for several years.

CBP's efforts in developing this initiative are in pursuit of a strategic objective that is not only mandated by the SAFE Port Act, but is highly logical in order to enhance containerized cargo risk screening.

The Congress, DHS, the Commercial Operations Advisory Committee (COAC), the Government Accountability Office (GAO), cargo security experts, and the industry all have recognized that reliance on carriers' cargo manifest data, while a fine start in developing effective security screening capabilities, has significant limitations. The present system provides either no or unreliable data regarding the commercial parties

[3] The ten cargo data elements of the new Security Filing have been identified by CBP as: 1) Manufacturer (or Supplier) Name and Address, 2) Seller (or Owner) Name and Address, 3) Buyer (or Owner) Name and Address, 4) Ship To Name and Address, 5) Container Stuffing Location(s), 6) Consolidator (or Stuffer) Name and Address, 7) Importer of Record Number, 8) Consignee Number, 9) Country of Origin, and 10) Commodity 6-Digit HTS Code.

involved in buying and selling the goods, where the goods are originating and who produced or supplied them, where the goods are ultimately going, and where and by whom the container was stuffed. The "10 plus 2" rulemaking seeks to address these shortcomings.

The comment period on the "10 plus 2" rulemaking recently closed. Many of the comments that have been submitted to CBP with respect to this rulemaking are in fact thoughtful observations and suggestions, identifying legitimate issues that warrant a clear government response. That is a positive attribute of the open and transparent rulemaking process that CBP has adopted in the development of this initiative. And, there is little question that CBP understands that this initiative is a substantial one that requires care and deliberation, that it requires significant changes to how U.S. maritime containerized import commerce is documented, and that it will require a gradual phase-in period and implementation process.

But for those who go beyond seeking specific answers or adjustments to the proposal to address specific concerns and make it work better, and seek instead to stop it from proceeding, what is the alternative cargo security strategy? Status quo reliance on carriers' bill of lading data for cargo risk assessment?

The "10 plus 2" rulemaking is the most significant initiative the Department of Homeland Security is currently taking to enhance its maritime cargo and supply chain security capabilities. It is a major rulemaking, and it is encountering some resistance within the trade community. It is an appropriate issue for Congress to monitor.

The Subcommittee has titled this hearing "Container, Cargo and Supply Chain Security – Challenges and Opportunities." Implementation of the "10 plus 2" initiative will certainly involve challenges; however, it is also the single greatest opportunity to enhance the government's capacity to conduct better informed supply chain risk assessment. Failure to proceed with this initiative to enhance cargo risk assessment capabilities would leave containerized cargo targeting limited to its present, limited data, and would fail to address the Congressional mandate to obtain better data. Failure to proceed would also likely give the government less capability and confidence to allow for the efficient continuation of commerce in the event that we ever face a security incident involving containerized cargo.

As CBP digests all of the comments it has received on the proposed rule, the most significant questions will not be questions about the format of specific data fields, or the definitions of specific terms, or the length of the phase-in implementation period, but the strategic question of whether and how the agency intends to improve its advance cargo risk assessment capabilities.

The World Shipping Council supports the "10 plus 2" initiative. It hopes that CBP will consider all the public comments, make whatever clarifications and adjustments to the rule may be appropriate, and proceed with a deliberative and reasonable implementation plan. A decision not to proceed with the "10 plus 2" initiative could easily raise even more difficult supply chain security strategy questions than what the trade faces today.

Global Trade Exchange (GTX): Another pending effort within DHS regarding the acquisition of additional cargo shipment information for enhanced risk screening is

less understood by the trade. Notwithstanding the fact that CBP has not yet even acted on its proposed "10 plus 2" regulations requiring additional information for cargo risk assessment, it has issued a Request for Information designed to commence an additional trade data gathering effort under the name of the "Global Trade Exchange" or GTX.

This development of this initiative has not been transparent or clearly explained to the industry. In fact, it has been shielded from scrutiny by the procurement process DHS has chosen to use.

The Department has not identified specific data it wants from GTX in order to improve security, apparently leaving such a fundamental question to potential vendors to address. DHS has stated that such shipment data would be shared with other governments, but it is not clear how, or whether, other governments want this service. DHS has not explained why trading enterprises should send confidential business data to a for-profit enterprise for submission to regulatory agencies, when such enterprises can file that information directly with the government themselves if the government wants it. How this system would be integrated into CBP's existing Automated Targeting System is unclear. How such a commercial third party data manager would make money off this program is unclear, and who would bear what costs for participating in such a system is unclear. What the uses of the data, other than assisting Customs with supply chain risk assessment, would be are unclear. How the data in the system would be protected is unclear. Whether ocean carriers would be expected or invited to participate in the provision of information is unclear. What benefit would result from participating in such an effort is unclear.

In short, the GTX effort has been hampered by poor dialogue with and understanding of the trade community. COAC wrote to the Secretary of DHS requesting consultation on this initiative, but no meaningful consultation was provided.

This Subcommittee might reasonably inquire whether taxpayer dollars are being expended wisely on this initiative. It may be a more effective use of scarce resources to use any money considered for obligation on this GTX project on the development and roll-out of CBP's Automated Commercial Environment or ACE system instead. That is an essential trade data system that the entire trade community understands and supports.

C. 100% Overseas Container Inspection Statute

In 2007, the Congress included in the "9/11 Commission Recommendations Act" provisions that appear to require overseas radiation and NII inspection of 100% of all cargo containers destined for the U.S. by 2012. The Council believes that this legislative mandate was not clearly considered and remains presently impractical. The WSC issued a statement on this legislation on July 30th, which is available on the Council's website. Our October 30, 2007 testimony before the House Homeland Security Committee also discussed some of the issues raised by these provisions.

In order to further consider the issues involved in the application of additional container inspection at overseas ports of loading, DHS has undertaken the "Secure Freight Initiative", under which pilot projects are being established at several foreign

ports testing more complete pre-vessel loading scanning, generating possible lessons to be learned for broader application of pre-vessel loading container inspection efforts.[4]

This is a worthwhile effort. While we are confident that many lessons may be derived from these pilots, we would hope that the current and future pilots might also be able to provide useful insights on the following questions.

First, the statute provides that containers are expected to be run through radiation detection equipment *and* non-intrusive imaging equipment before vessel loading. What, if anything, would be done with the images or data produced by those scannings was not addressed by the statute. The law requires that containers be scanned, but it does not require anybody to review or analyze the scanning data. This is a much more significant issue with respect to the NII images than radiation scanning; radiation scanning equipment can generate automatic alerts, whereas NII images require human analysis. These and future SFI pilots can help identify and address this set of issues, including relations between the host government and the U.S. government, identification of how and where the data is to be electronically transmitted, and what information technology and information systems issues arise in the collection, transmission and storage of the significant quantity of resulting data.

Second, the pilot projects can help identify another issue left unaddressed by the terms of the statute, namely who is to perform the screening data analysis task, and when and under what circumstances this is to occur. In some places, this may be CBP. In other places this may be the foreign Customs authority. We understand that the SFI pilot in Port Qasim uses U.S. government contractors to perform the remote screening and transmittal of data back to CBP's national targeting center. While one would expect that radiation scanning would be comparatively simple, the question of when and under what circumstances analysis of the NII scanning images would need to occur is an issue unaddressed by the statute.

Third, it is our understanding that the Congress did not intend that the overseas container scanning function was to be left to foreign companies (such as Dubai Ports World) to perform, but was to be a function of either the U.S. government or the sovereign government of a trusted trading partner. This is a key issue, particularly as some in the terminal operation business may be willing to explore installing such equipment if they could charge for the container scanning and make a profit from this activity. If this private approach were to be considered, then the government would need to carefully consider a number of questions, including the following: 1. Does the government see this as a private sector function, and if so, does it have criteria for who it would regard as acceptable to perform this function? 2. What would be the necessary operating standards and protocols for private sector companies to perform this function? 3. What is the security function that the foreign terminal operator is to perform? Does it perform any action other than operating scanning equipment, transmitting the resultant data to governments, and collecting a fee for the service? 5. To whom can it provide or sell the data that is generated? 6. Who pays for the data transmission costs? 7. What would CBP do with all the data it receives, since there is still no automated way to

[4] DHS has established three full scale container scanning pilots in co-operation with host governments at Southampton, U.K.; Puerto Cortes, Honduras and Port Qasim, Pakistan. Three other smaller scale pilots are under development at port facilities in Busan, South Korea (Gamman Terminal); Salalah, Oman, and Singapore.

analyze NII images? 8. If the terminal operator pays for and installs the scanning equipment, which functions does the government retain? 9. What happens to smaller ports that do not have such scanning equipment – are they required to transship their goods through ports that do?

These and future SFI pilots can help identify the capital and the operating costs of establishing the necessary capability to perform the task of 100% container scanning, and what portion of the costs is to be borne by CBP, what portion is to be borne by the U.S. Department of Energy, and what portion is to be borne by foreign governments. The entire set of necessary "system" costs can be further analyzed and understood through such SFI pilots. For example, we understand that in one of the second set of SFI pilots currently underway, it has been estimated that the cost of simply transmitting the data files to the U.S. amounts to roughly $500,000.00 per month.

Fourth, these and future SFI pilot programs may shed additional light on the extent to which the government of the United States' trading partners will expect the U.S. government to perform such scanning of its own export containerized cargo on a reciprocal basis. We note that no pilots have yet been established to test the effects of such a concept at U.S. ports.

Fifth, we recognize that the first three SFI pilot programs chosen were at relatively low volume ports with little, if any, transshipped containers. While the Council understands and has no criticism of starting these SFI pilots with low volume ports whose trade flows are relatively simple, these pilots will not shed light on what kinds of issues would be encountered at high volume ports or at ports with significant volumes of transshipped containers that do not pass through the marine terminal gates.

How 100% container scanning could be performed on transshipped containers remains an unanswered question, but one that is of critical interest both to major transshipment ports, such as Singapore, and to cargo that is transshipped. The container volumes being handled at major transhipment terminals can approach 10,000 containers per day on peak days. Furthermore, when a container that is to be transshipped onto a U.S. destination vessel is discharged into a port facility, that facility often does not knows with certainty that the container will be U.S. destined cargo, creating significant operational uncertainties and challenges. The "lessons learned" from the initial SFI pilots will not be sufficient to address those challenges.

The point of these observations is not to criticize the existing or planned SFI pilots in any way, but to note that care must be applied in determining what the "lessons learned" are from these initial pilots, and to note that simply because a small scale pilot at one port may encounter no substantial difficulties does not mean that the concept of 100% container scanning is ready for implementation at all ports. Even for containers entering a terminal by road, the container screening capacity has to be gauged to the size of the terminal, the peak periods, and the opening hours – all of which has a significant impact on the number of hourly truck visits the facility will have. In addition, the response time has to very short. The processing time of the truck will determine how many gate lanes and screening portals will have to be installed.

Sixth, we note that there is some ambiguity in the 100% container scanning statutory language, about whether the non-intrusive container scanning of all containers

is a requirement, or whether the statute might be construed in such a way as to require 100% radiation scanning only. This too is a key issue, and it is affected both by an assessment of the effectiveness of radiation scanning equipment at detecting nuclear and radiation risks (i.e., if radiation scanning by itself is not adequate, then is NII scanning and analysis necessary?), and by the enormous impediment to trade that would result from a requirement that NII images of every cargo container be analyzed by a trained imaging expert prior to vessel loading. In this regard, we note that the World Customs Organization (WCO) Secretary General, in a December 13, 2007 letter to Senator Lieberman, Chairman of the Senate Committee on Homeland Security and Governmental Affairs, supported "well-reasoned risk management systems" and the use of NII scanning to assess the potential risk of containerized cargo which has been identified as questionable by such risk management systems, in contrast to NII scanning of all containerized cargo. He went on to note that: "the WCO raises no objection to another requirement present in the new United States law, namely that all containerized maritime cargoes be subjected to radiation detection processes prior to shipment." The Secretary General appears to be suggesting that 100% radiation scanning of containerized cargo might be an appropriate alternative strategic vision, when backed up by NII inspection of those cargo shipments that have been determined through risk assessment to present security questions. This is a proposition that warrants further consideration.

Seventh, we note that U.S. statutes and regulations do not specify the technical standards that either the radiation or the non-intrusive scanning technologies must meet. We would expect that this issue is one that the present and future SFI pilots could further develop. We also note that in major transshipment ports, 100% container radiation scanning may require the use of crane mounted scanning equipment. Future SFI pilots might be an appropriate mechanism to explore such technology and provide technology vendors greater clarity about the technical specifications that such crane mounted, radiation scanning equipment would need to meet.

Eighth, we note that significant questions exist regarding the timing and availability of data to facilitate the NII screening of containers. The NII cargo images are assessed, analyzed and matched against manifest information and other pertinent information that may be available. Manifest information may not be available when the container arrives at the port terminal location where the scanning is completed. This issue can be addressed more fully in the pilots.

Ninth, additional SFI pilots may help address the challenges that will arise at many ports of segregating U.S. destination containers from non-U.S. destination containers that will not need to undergo the container scanning.

Tenth, additional SFI pilots will allow CBP to obtain better information about the impacts on port terminal productivity and about delays to cargo shipments arising from 100% container inspection.

Eleventh, the SFI pilots will need to address the issues of who needs to know that the container has been scanned, and how would they know it.

Finally, we understand that in trying to determine how one would actually perform 100% NII screening of containers, some consideration may be given to performing this function at a place or facility that is separate from the port of loading. We recommend

that any pilots considering this approach should do so with some care and clarity, as this approach could add another layer of costs, delays and operational difficulties above and beyond the scanning of the box, including additional drayage, and including additional layers of security measures to be applied from that remote scanning location to the port of lading. The ancillary costs and operational complications from these issues could be at least as significant if not greater than the problems and costs arising from the scanning of the cargo shipments.

In summary, radiation and NII scanning of container cargo can provide significant security value, and the Council supports CBP's present strategy regarding the deployment and use of such technology. The concept of 100% mandatory overseas container scanning requires numerous significant issues to be addressed if it is to be considered as a security goal.

D. Container Security Technologies

Container Scanning Technology: The most important technologies being applied to containerized cargo security are the radiation scanning and the NII scanning of containers discussed earlier. The earlier discussion in this testimony of this issue focused on the "who, when and where" issues related to the use of such technology.

Another set of important questions are the technology standards for such scanning equipment and the equipment's effectiveness.

We recognize that different types of equipment, from different manufacturers are being used, and we are aware of the strong interest of some to develop container crane mounted radiation scanning equipment that may be determined to be acceptable and withstand the rigors of that operating environment. The Council does not have the technical expertise that CBP, the Office for Domestic Nuclear Detection, and the Department of Energy have on these subjects. We expect that the Subcommittee has endeavored to satisfy itself that the appropriations for such equipment are being used for equipment that meets appropriate levels of effectiveness.

Container Sealing: The "9/11 Commission Recommendations Act" provides that: "effective not later than October 15, 2008, all containers in transit to the United States shall be required to meet the requirements of International Organization for Standardization Publicly Available Specification 17712 standard for sealing containers…." We expect to work closely with CBP to ensure the effective implementation of this requirement within the required time frame.

"*Conveyance Security Devices" (CSDs)*: CBP has announced that it plans to conduct various pilots that will test "conveyance security devices" in a number of different settings where they may provide useful information. The Council supports the agency's efforts in this regard, because these kinds of devices are not "miracle cures" and their limitations as well as their potential benefits need to be carefully considered and tested.

Some of the questions include the technical requirements for such devices. CBP has issued specifications for devices for their initial pilots. These and future

specifications must address issues such as: what specifically the device would be required to do and its security value, what acceptable false positive and false negative reading rates would be, what radio frequency would be used, the requirements for the installation and operation of the necessary device reader infrastructure, the requirements applicable to the necessary communications interface and protocols with CBP, the security vulnerabilities of such devices, the necessity of interoperability of various vendors' devices and systems, the data to be captured and transmitted by the device, identification of who will have access to the data in the device, survivability and vulnerability of the device, power or battery life requirements, the probability that the device can be detected or removed without detection, required data messaging formats, event logs, and data encryption.

These questions are even more complicated in the environment of international maritime commerce than they would be in a more controlled environment of U.S. border stations where CSD reading infrastructure would be under the sole control of CBP.

Finally, the operational protocols that would be needed for effective use of such devices need to be analyzed and considered. For example, in some trade lanes, foreign Customs authorities will open the doors of most containers before they leave the country, meaning that such CSDs will all alarm. What operating protocol would be applied in such situations?

In short, the CBP pilot programs will begin to shed some useful light and analysis on a wide array of questions that would have to be addressed in considering the application of such technology.

IV. Conclusion

Vigilance against terrorist risks requires the development and implementation of prudent security measures, and the continuing enhancement of such measures as the risks change and take new forms.

The liner shipping industry fully understands this and has cooperated with national governments and international organizations trying to construct meaningful security regimes. The industry will always be concerned that these measures not unduly delay or restrict commerce or impose costs that produce little added security; however, it has supported and will continue to support measures that are well designed and provide real security value.

We believe CBP does an excellent job trying to address this most complex challenge, and we appreciate this Subcommittee's continued interest and oversight of these issues. We would be pleased to provide additional information that may be of assistance. Thank you again for the opportunity to testify.