Testimony of

Christopher Koch

President & CEO
World Shipping Council

Before the

House Homeland Security Committee
Subcommittee on
Border, Maritime and Global Counterterrorism

"SAFE Port Act: Status of Implementation"

October 30th, 2007

I. Introduction

Good afternoon and 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 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 95% 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 1,000 ocean-going liner vessels, mostly containerships, make more than 22,000 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 70 percent of the $700 billion in U.S. ocean-borne commerce is transported via liner shipping companies.

The international liner shipping industry has been determined by the Department of Homeland Security 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. The Focus on Maritime Security

For the past six 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 $1.3 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 multi-layered maritime security strategy has a number of parts on which I will briefly comment today. 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 (ISPS). Second, there is *personnel security*, overseen by various Department of Homeland Security agencies and the State Department. Third, is *cargo security*, which with regard to containerized cargo, is addressed through Customs and Border Protection'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.

A. Vessel and Port Security Plans

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 no 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: On October 3, 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 objective and the enhanced visibility of vessels offshore that it will give to the Coast Guard and other governments.

The Coast Guard expects existing maritime satellite communications equipment to be able to meet these tracking requirements. Assuming this is correct, the Council does not foresee major problems complying with these regulations.

The LRIT system is based on a network of data centers sharing information. A vessel will transmit its data to the data center selected by its flag administration. This data center could be a national center, like in the U.S., a regional or cooperative center, perhaps like the European Union, or an international center, open to any country to join. Coordinating the sharing of information between the data centers is an International LRIT Data Exchange (IDE). The IDE is the body that is connected to all other LRIT data centers and routes information between LRIT data centers. The IDE shares information in accordance with the LRIT Data Distribution Plan.

There may be concern, however, regarding how the Coast Guard intends to implement LRIT if the International Data Center (IDC) is not in place. The IDC is where a vessel whose country of registration has not established its own data center is to send its position reports. Many smaller nations were expected to use the IDC and how their vessels will comply with the LRIT requirements is in question. An agreement has been reached to allow the Coast Guard to host the International Data Exchange (IDE) on an interim basis until January 1, 2010. It is unclear what happens with the IDE after that date. A uniform, global operating system is the desired objective. The Coast Guard has invited comments on these issues in its recent NPRM, and we expect that the industry and other governments will be considering these issues closely.

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 effort are focusing on a legitimate concern. We also appreciate that the U.S. Coast Guard is playing a lead role in having put this on the International Maritime Organization's agenda in order to develop international principles and criteria for addressing this issue.

B. ***Transport Worker Identification Credential***

The Council supports the credentialing of maritime 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 Transportation Security Administration on the development of the TWIC regime. The industry's primary concern is that the security enhancement envisioned in this new system not have undue impacts on those personnel who work in port terminals servicing vessels or on port operations.

The SAFE Port Act requires TWIC reader pilot projects to be run in at least five locations. NMSAC has recommended that the final TWIC regulations should not be published until the results of these pilot projects are known.

The Coast Guard has indicated its intention to issue two sets of proposed rules on the TWIC regulations: the initial set to give some shape to the pilots and the second, supplemental proposal which is intended to finalize the proposed regulations when the pilots' results are known. We support this measured approach.

The Coast Guard also recently announced the biometric standard to be placed on the TWIC card. This standard contains two items that were not supported by the industry: encryption and a Personal Identification Number (PIN). The industry's concern has been that encryption will create operational complexities which have the potential to severely impede the flow of maritime commerce. Further, the NMSAC does not believe the significant additional costs associated with encrypting the fingerprint template are warranted given the minimal risk involved without such encryption. How these two items will work with readers remains to be seen, but the industry is hopeful that the good consultative process that the Coast Guard has established with NMSAC will allow for these issues to be addressed satisfactorily.

Lastly, DHS has begun to enroll workers in Wilmington, Delaware, and has also listed the next eleven follow-on locations for enrollment. The industry strongly supports a measured implementation of this challenging new regime so that any unanticipated issues that may arise can be addressed as the system is rolled out in stages.

C. Containerized Cargo Security

The WSC fully supports the U.S. government's strategy in addressing containerized cargo security. Specifically, the Council supports CBP's risk assessment and screening of 100% of all containers prior to their being loaded onto vessels destined for the U.S., and the pre-vessel loading inspection of 100% of those containers that CBP's cargo risk assessment system determines to present a significant security risk or question.

The Council does not support recent legislation's call for inspection of 100% of all import containers before vessel loading, because the concept has not been clearly considered and remains presently impractical.

1. Container Security Initiative (CSI)

The network of bilateral Customs-to-Customs agreements forming the "Container Security Initiative" (CSI) continues to grow. There are now 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.

The United States' approach to supply chain security up until now has been dominated by an interest in inbound or imported cargo. This is understandable, but as supply chain security regimes become more globalized, and as our trading partners call for "reciprocity" and "mutual recognition" of security improvements, it is very important that the Department of Homeland Security plan for and implement a coordinated strategy for dealing with the nation's international import and export maritime commerce.

When CBP calls for a foreign Customs authority's assistance to check a container it has a question about before vessel loading, so must it plan and be able to act on that same foreign Customs' authorities request for assistance on checking a U.S. export container that may raise a question. When discussing with foreign governments "mutual recognition" of supply chain security protection programs, the U.S. government will be called on to address what programs enhance the security confidence of U.S. exports to the same extent that other governments' programs enhance the security confidence of their exports. We believe that Customs and Border Protection is the right agency for establishing and ensuring a consistent and coordinated U.S. approach to such issues, and that additional planning should be undertaken in this regard.

It is for this reason that the Council recently wrote to CBP to recommend that the agency plan for how to expand its CSI Customs-to-Customs cooperative partnerships with European customs authorities to prepare for the planned 2009 implementation of the European 24 Hour Rule under Commission Regulation 1875. The purpose of such planning would be to ensure that American export commerce receives the same kind of cooperative and expedited consideration when European authorities raise security questions, as European export containers receive today when CBP raises such a question.

We also note that, 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 still prevent 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.

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

24 Hour Rule: Another important element of the 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 in the Council's view a logical and sound effort, the Council has for several years noted 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, the SAFE Port Act sets forth the following requirement to enhance the capability of CBP's 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*."

Customs and Border Protection (CBP) is developing a regulatory proposal that would require U.S. importers or cargo owners to file ten additional data elements[2] with CBP 24 hours prior to vessel loading, and to require ocean carriers to provide two

[2] 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.

additional sources of data -- vessel stowage plans prior to arrival in the U.S., as well copies of electronic container status messages. This is referred to as the "10 plus 2" initiative.

CBP has undertaken extensive, transparent, and open consultation with the trade and carrier community in developing this proposal. It is our understanding that the proposed regulation to implement this new requirement should be published in the Federal Register for public comment in the near future, with implementation beginning sometime in 2008.

While the private sector obviously needs to await the actual proposed regulation before providing comments in the expected rulemaking, we would note that CBP's efforts in developing this initiative have been transparent, professional and cooperative, and 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.

Global Trade Exchange (GTX): Other pending efforts within DHS regarding the acquisition of additional cargo shipment information for enhanced risk screening are less understood by the trade. Notwithstanding the fact that CBP has not yet published, let alone implemented, its proposed "10 plus 2" regulations requiring additional information for cargo risk assessment, DHS officials have indicated that the Department will be proceeding with efforts to commence an additional trade data gathering and analysis effort under the name of the "Global Trade Exchange" or GTX. This initiative has not yet been clearly explained to the industry.

What we understand at the present time is that DHS is considering awarding funding for an initial phase of this initiative. It is our understanding that participation by members of the trade providing such additional data is expected to be voluntary, that the party to collect the data would be drawn from a restricted number of commercial entities acting as a third party data clearinghouse, and that secure and confidential treatment of any data provided is recognized to be needed.

What services, analysis or risk assessment competence would be required of such vendors is unclear. What the specific data to be gathered would be has not been explained. The extent to which such shipment data would be shared with other governments is not clear. 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.

DHS has indicated that the intent is to proceed under a "request for quotation" solicitation process, which is restricted to a limited number of vendors now established in the DHS "EAGLE" procurement program.

In short, the GTX effort has not yet been explained by the government and is not yet understood by the trade. U.S. importers with whom the Council has discussed this

initiative are confused by this process. There is some concern within the trade community over the apparent development of such an initiative without the government's usual transparency and process of consultation. COAC has written to the Secretary of DHS requesting consultation on this initiative.

3. Container Inspection

DHS has a well established strategy to undertake radiation scanning of all containers entering the U.S. before they leave a U.S. port. CBP recently deployed its 1000th container radiation portal monitor as it gets closer to its objective of performing radiation scanning on 100% of all inbound containers at U.S. ports of discharge.

CBP also undertakes non-intrusive inspection technology (NII) or physical inspection of 100% of all arriving containers that are determined to pose a significant security question. CBP has no plans and no capability, however, to inspect every arriving container. Because that is not practical, the agency is utilizing, and soon will be enhancing, its cargo risk assessment system and the CSI program to identify which containers do warrant inspection.

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.[3]

The "Implementing the 9/11 Commission Recommendations Act", which was signed into law in August, includes the well known provision requiring that by 2012 100% of the containers imported into the United States be "scanned" before being loaded aboard vessels destined for the United States, meaning that the container would have 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 law, nor were a host of other highly relevant questions, including who was to perform this task, and whether the U.S. would perform such scanning of its own export containerized cargo. The WSC issued a six page statement on this legislation on July 30th, which is available on the Council's website.

Many foreign governments are obviously and justifiably concerned about the implications and meaning of this new U.S. law. We expect that they will continue to inform the U.S. government of their concerns, including their view that this statutory provision expects foreign governments to undertake measures for their exports that the U.S. government has no intention to undertake for its exports.

The shipping industry's customers -- the hundreds of thousands of U.S. importers and exporters who use containers to transport their cargo -- are also concerned about

[3] 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.

the meaning and potential effects of this law. The port terminal operators around the world that service the industry's vessels are also concerned but unsure about the intent or effect of this statute.

Several things seem clear. First, implementation of this law's stated objective would require addressing many serious issues that the statute does not address, including the fact that implementation of overseas container inspection requires the cooperation of foreign governments. Second, the U.S. government has no current plans to scan 100% of its outbound export cargo containers, and thus foreign governments' predictable inquiries about reciprocity will likely be unanswerable. And, if the United States' trading partners do not implement 100% container scanning, there is nothing that the U.S. government can realistically do about it other than cease trading with the rest of the world. We therefore see the obvious need for further international dialogue on this matter.

At this time, this provision of the "9/11 Commission Recommendations Act" is an indecipherable riddle. The world has no idea what to make of it and does not know if it expresses the real strategy of the United States or not.

If the Congress intends to pursue any kind of meaningful dialogue or progress on determining what would need to be addressed in order to pursue this statute's stated vision of 100% container screening at foreign ports, then we respectfully submit that it should begin to consider and address a number of critical questions, including the following:

1. Whom Does the Law Intend To Perform the Container Scanning? The legislation pointedly fails to address the issue of who is to perform this activity. It does not require U.S. Customs to do this, as it is clearly impossible for the Congress to require U.S. Customs to undertake such activities within the jurisdiction of other sovereign nations. It does not require foreign governments to do so, as it has no such authority. The legislation simply says that containers shall be scanned. By whom? Who is to purchase, operate and maintain the equipment?

   Is this a sovereign function to be handled by governments? Is this a private sector function? Before private marine terminal operators could seriously consider such an investment and activity, the Congress would need to provide clarity on this point and who would be trusted to perform the task and under what circumstances.

   Does Congress intend that non-government foreign port facility operators would perform this task? The 109th Congress took the position that one of the largest port facility operators in the world, Dubai Ports World, was an unacceptable security risk to buy a U.S. marine terminal operating company and hire U.S. workers, working under U.S. management, to service vessels in U.S. ports. Would Congress consider that company acceptable to perform this task in foreign ports? The largest terminal operating company in the world, Hutchison Whampoa, is owned and controlled by the Chinese. Would Congress consider that company acceptable to perform this task?

   Even if the Congress were to determine that such terminal operating

companies were appropriate entities to install and operate the necessary scanning equipment, and even if these companies were willing to make the capital investments necessary to install and operate this equipment, the law fails to answer who will review, interpret and analyze the readings produced by the technology. It is extremely unlikely that these terminal operating companies would accept the responsibility or the liability for the actual analysis and assessment of the scanning technology.

2. Failure to Define the Scanning Requirement: Recognizing that 100% container "inspection" is impractical, the statute requires instead that every container be "scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel." This by itself would be pointless.

   The law fails to address whether the scanning data actually has to be reviewed and analyzed, and if so, under what circumstance, when and by whom? The law fails to address whether or when the data from the scanning equipment is transmitted to the U.S. government and at whose cost. There are many complexities and costs involved in addressing these issues.

   Is every container radiation scan to be reviewed before vessel loading, with mandatory secondary inspection if there is an unusual radiation reading?

   Is every NII scan to be reviewed before vessel loading? Or, is it only those containers that trigger a certain threshold in CBP's Automated Targeting System that require review of NII scans? If only a few percent of the containers would have their NII images reviewed before vessel loading, what is the point of requiring 100% of all containers to have NII images? Why not just perform NII inspections on the containers that present security questions?

3. No Reciprocity: The statute purports to require 600 ports around the world to approve, implement, and utilize such technology, systems and processes for all cargo destined for the U.S. or effectively face an embargo on their exports, when the U.S. government does try or plan to perform this function on its export cargo, and scans virtually no U.S. export containers. If implementation of this law were actually pursued, it is entirely possible, if not highly likely, that foreign governments would establish "mirror image" requirements on the U.S., forcing all American export containers to undergo radiation and NII scanning before vessel loading at U.S. ports -- requirements which the U.S. government and U.S. port facility operators are presently and for the foreseeable future incapable of meeting. Is the Congress prepared to fund such a system for U.S. exports?

4. Threshold Technology Question: The statute provides that DHS may "extend" or waive the scanning requirement, if: "(F) Systems to scan containers in accordance with paragraph (1) do not adequately provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel." NII container inspection technology does not have any government or commercially accepted software that enables "automatic notification of questionable or

high-risk cargo", putting aside the relevant question of defining what would constitute "questionable or high-risk cargo" that the technology would need to identify. Does this mean that until NII equipment can meet such a standard that has yet to be defined and agreed upon, that this statutory mandate is not applicable?

The "9/11 Commission Recommendations Act" provisions calling for 100% overseas container scanning has raised more questions than it has answered.

4. Seals and Container Security Devices

The SAFE Port Act included the following directive: "Not later than 90 days after the date of enactment of this Act, the Secretary shall initiate a rulemaking proceeding to establish minimum standards and procedures for securing containers in transit to the United States." (Section 204(a)) It was not evident what this provision meant or how it might be interpreted, and the section's time deadlines were not going to be met.

Accordingly, the "9/11 Commission Recommendations Act", Congress amended this section by providing that: "(B) Interim Requirement.-- If the interim final rule described … is not issued by April 1, 2008, then .... 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…." Thus by next October, all U.S. inbound containers will be required at a minimum to have ISO standard security seals. This provides helpful clarity.

As to the government's view of "container security devices" (CSDs), things are less clear. First, CSD is not a defined term. For example, some say that a seal is a CSD; some say a seal is not a CSD. The Council has understood that DHS was planning to issue proposed draft technical requirements for container security devices and the operating protocols associated with such devices by the end of this year for public review and comment. We understand that the DHS Science and Technology directorate prepared a draft of such requirements that is undergoing further review and amendment within the Department.

The Council and other members of the trade have requested that CBP/DHS allow for full transparency into the development of this effort and solicit public comments on the draft requirements, after they have completed internal government review.

There are at present many unanswered questions about CSD requirements, including 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.

The Council believes it is essential, if an interest in CSDs is to be pursued, for the government to undertake a fully transparent and very clear articulation of its draft views on the requirements for such technology and the related operating systems and protocols, and to provide the public with a meaningful opportunity to comment upon such draft requirements, *before* they are advanced as an element of the government's container security strategy.

III. 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 international trading system is too valuable and important to be left unattended.

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 with as little impact as possible on legitimate trade.

This is clearly difficult work, but there are clearly some success stories. The International Maritime Organization's development of the International Ship and Port Facility Security (ISPS) Code, the Proliferation Security Initiative, the Container Security Initiative, the "24 Hour Rule" advance cargo screening strategy and its imminent enhancement, the C-TPAT program – all have enhanced supply chain and maritime security. The government's expanded use of container inspection technologies is another example of sound strategy and implementation.

If we are to continue to make progress in enhancing maritime and supply chain security, progress is more likely to occur if:

1. There is a clear and specific definition and agreement on what should be done to improve security.

2. There is a clear and thoughtful prioritization of initiatives.

3. There is sufficient certainty and clarity in purpose to do it right. In the absence of that, time and resources are poorly used and the efforts are less likely to improve security.

We appreciate the Subcommittee's continued interest and oversight of these issues, and would be pleased to provide additional information that may be of assistance to the government in addressing these issues. Thank you again for the opportunity to testify.