



WORLD SHIPPING COUNCIL
PARTNERS IN TRADE

Remarks of

Christopher Koch

President & CEO

World Shipping Council

Before the

Maritime Security Expo 2006

New York City

September 19th, 2006

I appreciate the opportunity to address this fifth annual Maritime Security Expo and provide some comments on the state of maritime security initiatives and the international liner shipping industry.

2006 has demonstrated that world trade volumes continue to grow at a rapid pace, that the transportation infrastructure handling these volumes is often operating at or close to capacity, that further efficiencies, speed and investment are needed to handle future trade volumes, and that the efforts and the need to enhance maritime and containerized cargo security are a continuing obligation and challenge.

In the limited time available this morning, I would like to briefly touch on security policy developments in both the U.S. and in the European Union.

I. U.S. Developments

Maritime Security: 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 in regards to containerized cargo is addressed through the well-known “three legged stool” of Customs and Border Protection’s 24 Hour Rule 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.

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 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.

Personnel Security: Personnel security is one of the more active areas of DHS attention and development, for fairly obvious reasons. The most significant and difficult new undertaking in this regard is the Transport Worker Identification Credential (TWIC).

Before touching on that, I would like to briefly address the continued criticism from some quarters of the U.S. government's treatment of seafarers, its unwillingness to accept the recent ILO Convention's seafarer credential, and its insistence on an individual visa for seafarers who wish to enter the country.

The fair and humane treatment of seafarers is an important issue and deserves serious consideration by industry and government. However, it is no more correct to argue that the government is characterizing seafarers as "potential terrorists" than it is to say that the government is treating all 11 million nonimmigrant visitors to the U.S. from non-visa waiver countries as "potential terrorists". All such persons, plus any foreign individual in the U.S. for work or educational reasons, are required to be in possession of individual visas that are issued after personal interviews and the collection of biometrics at U.S. diplomatic posts. The government, as directed by U.S. statutes, is requiring visitors to have proper government credentials for entry into the country, and is improving its monitoring of people entering and exiting the country through the US VISIT program as strongly advocated by the *9/11 Commission Report* and other security advisors, while at the same time trying to address the potential terrorist threat to shipping.

In the last three years, nearly 700 persons have illegally entered the U.S. as seafarers illegally absconding or deserting their ship. While it is true that this number may be less than the number of people illegally crossing the Mexican border in a day, it is also true that the maritime industry has shown itself to be a potential vector of illegal immigration. Nations do have a legitimate interest in trying to devise effective ways to check who is crossing their borders. In that regard, a foreign seafarer is not different from a foreign airline pilot, businessman, student or artist.

Seafarers have been clearly advised by the government to obtain visas in order to obtain shore leave. That requirement is unlikely to change. Those who do have valid visas are generally treated professionally and courteously, and given shore privileges. For those who do not have visas, the U.S. government has made it clear that the proposed ILO seafarer credential cannot become a substitute for a visa. The government has made that determination because of the biometrics used in the credential, and the government's insistence that personal interviews are essential for screening out undesirable foreign visitors.

Because liner shipping vessels operate on regular schedules, their crews know in advance if they are coming to the U.S. and whether they will need a visa. For those seafarers aboard vessels who do not know the vessel will call at the U.S. until after they sign on and do not have the necessary visa, one can and should sympathize with their desire to obtain shore leave when they arrive. As a way to try to address this concern, the State Department has stated that seafarers, who don't know for certain but may be working on ships that will call at U.S. ports, may apply for a visa. Improving the lot of these seafarers will require new ideas and a cooperative environment for the exchange of such ideas. The Council welcomes that the State Department has started an outreach to industry about these issues, and we are committed to offer our assistance wherever needed and relevant.

For U.S. shore-based maritime workers, the current initiative by the Coast Guard and the Transportation Security Administration (TSA) to devise and implement the TWIC system involves one of the more difficult and important maritime security challenges the industry has faced in recent years. Making sure that every port worker, every truck driver, and every other regular employee entering a secure port area has a proper TSA approved security credential that can be efficiently and effectively read, under normal maritime operating conditions, with appropriate biometrics, matched against appropriate data bases is an enormous task. To devise such a system that can work in all of the various maritime industry sectors, from offshore oil and gas, to inland waterways, to seasonal industries, to container terminals will require a close and cooperative partnership of industry and government.

The liner shipping industry and the marine terminal operators who service the liner shipping industry have all consistently supported the TWIC concept and its implementation. However, as the National Maritime Security Advisory Committee recently advised the Department of Homeland Security, this program must be implemented carefully and correctly the first time. Addressing the technology issues associated with the TWIC and the TWIC readers, increasing the clarity of who must obtain a TWIC, and addressing the various real world implementation issues that different sectors of the industry face will require a steady, careful implementation and dialogue with the industry.

Container Security: CBP's basic container security strategy – to perform cargo shipment security risk assessment before vessel loading, to cooperate with the governments of trading partners through agreements negotiated via the Container Security

Initiative, to enhance security of supply chains via C-TPAT, and to scan all arriving containers for radiation and to inspect any other shipment considered potentially risky with non-intrusive technology – is fundamentally sound.

It also must mature and improve. How and in what way should that occur? Two improvements under development and review are entirely appropriate, needed and important. One is the acquisition of better cargo shipment data for cargo screening and risk assessment. Another is the expanded piloting and use of radiation and density container inspection technology.

1. Improving Risk Assessment Data: The DHS strategy of using risk assessment and targeting techniques to review all containerized cargo shipments before vessel loading is logical from a security, an operational, and a practical perspective. The liner shipping industry fully supports it. But the Congress, DHS and the industry all recognize that reliance on ocean carriers' cargo manifest data, while a fine start, has substantial shortcomings. The present system provides either no or unreliable data regarding the commercial parties 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 data submitted to the government's cargo risk assessment system should be enhanced. Cargo manifest data should be supplemented in order to provide better security risk assessment capabilities. Currently, there is no data that is required to be filed into the government's container shipment targeting system by the U.S. importer or the foreign exporter that can be used in the pre-vessel loading security screening process. This occurs, even though these parties or their agents possess shipment data that government officials believe would have security risk assessment relevance that is not available in the carriers' manifest filings, and notwithstanding the fact that the law requires the cargo security screening and evaluation system to be conducted "prior to loading in a foreign port".

Accordingly, CBP has been working on an initiative to improve its targeting and risk assessment capabilities – the so-called "10 plus 2" initiative, because it would require 10 data elements to be submitted by importers or their agents 24 hours before vessel loading, and 2 additional data streams from carriers or their agents.

Implementation of "10 plus 2" would not be simple or cost-free, but the security logic of the proposal is obvious. A system that bases the nation's container security screening strategy on the information in a carriers' bill of lading will continue to be the subject of legitimate criticism from Congress, the Inspector General, Government Accountability Office, and anyone else performing a critical analysis of present security tools.

There are some challenging issues to make this plan a success, including:

- Developing clear definitions of the data to be provided (e.g., Is it the “manufacturer” of the goods or the “supplier” of the goods?),
- Determining what Customs information system will be used for the transmission of the data to CBP?
- Determining who will be authorized and trusted, and under what criteria, to submit the shipment data into Customs data systems?

As CBP continues to develop the specifics of this proposed concept, it will be important for the various parts of the import business community to come together in a way that will help CBP make this program a success.

Ocean carrier members of the Council have already begun pilot efforts with CBP on the “2” data streams of interest to CBP from the maritime sector.

A final point regarding this initiative is its relationship to trade continuity in the event of a transportation security incident involving containers. While this initiative is needed to improve the government’s ability to detect security questions and to prevent them from disrupting commerce or threatening populations, it could also be very important in the event the government had to manage the consequences of a major maritime security incident involving a container. The “10 plus 2” initiative would greatly enhance the government and industry’s ability to analyze and respond to what may have happened, and to determine what trade may be allowed to continue – an issue the trade community insists is a priority concern. If the trade community wants the government to allow its imports to face little delay in such difficult circumstances, it should make a priority of determining how to provide the government with the additional data it will need to be confident of the security of the cargo shipments.

While “10 plus 2” will not solve all containerized cargo security concerns, there is no convincing reason for CBP’s pre-vessel loading container risk assessment system to continue relying on the limited information it has access to today.

2. *Improved Container Inspection Capabilities:* CBP and the Department of Energy’s Megaports project deserve considerable credit for the effective improvement and expanded deployment of container inspection technology without substantially disrupting the flow of commerce.

With respect to the priority risk – detecting radiological and nuclear materials -- CBP’s strategy is to perform radiation scanning on virtually all containers entering the U.S.. Presently, roughly 68% of inbound ocean containers are scanned for radiation, and CBP expects to get that to close to 100% by the end of next year. In addition, DHS is working to improve the quality of the radiation detection equipment being used, with its July announcement of the award of Advanced Spectroscopic Portal (ASP) program contracts totaling \$1.157 billion to enhance the detection of radiological and nuclear material.

In addition to the objective of scanning all containers for radiation, CBP performs a density image inspection of all containers that its container targeting system identifies as presenting any significant potential risk using non-intrusive inspective (NII) equipment.

Thus, the government is making substantial progress on its objective of inspecting every inbound container for radiation, and every container that its targeting system says may present a security risk with an NII or physical exam.

The obvious limitation of these efforts is that the vast majority of these inspections are occurring after the vessel and cargo are in the U.S. at the port of discharge, whereas the ideal state would be for any such inspection to occur before the container is loaded aboard a vessel.

It is for that reason that the Department of Homeland Security, with the support of Congress, is moving ahead with increased pilot testing of its advanced overseas screening initiative, which will seek to undertake radiation and NII image capturing of all containers before vessel loading at select foreign marine terminals.

This too is a laudable strategy and direction. The “pilot” done to date -- which most observers know as the Integrated Container Inspection System or “ICIS” operated at two Hong Kong marine terminals -- provided a public relations boost to the concept; however, it did not even try to address the difficult, real world operational issues that hopefully this next round of pilots will begin to address.

ICIS captured images from Radiation Portal Monitors and NII equipment of the containers entering the terminal gate, but did nothing with them. No analysis of the images was performed. No actions were generated. No transshipped containers were scanned. No containers were delayed or had follow-up exams. No space in the marine terminal had to be set aside for secondary inspections. No demands on the foreign customs authorities to inspect containers were generated. No protocols with the host government were negotiated.

The promise of the advanced overseas screening initiative pilots is that they can analyze and try to address the realities that would arise from the concept’s real world implementation, namely:

- Negotiating the necessary agreements and protocols with the host government customs authorities
- Agreeing how to efficiently address and resolve radiation readings or other questions about shipments prior to vessel loading – a common occurrence
- Addressing health and safety issues involved in the deployment of such technology
- Addressing terminal operator liability and cost acceptance, and
- Determining how to efficiently scan transshipped containers that don’t enter the marine terminal via a gate, such as transshipped cargoes.

3. Why Are These Container Security Initiatives Important?

On any given day, on average, approximately 370,000 containers of cargo are loaded aboard vessels that are underway and enroute to the U.S. Those containers and the ships they are on utilize approximately *one-third of all the vessel capacity* serving U.S. international containerized commerce. If the government does not have confidence that the pre-vessel loading security screening of containerized cargo under the “24 Hour Rule” is adequate, and the vessel capacity bound for the U.S. were to have significant restrictions placed on its operations because of security concerns about containers that have already been permitted to be loaded onto them, there would be substantial, adverse consequences to the import and export transportation network and global supply chains. Furthermore, for every day the government cannot provide assured instruction regarding what can be reliably loaded onto and discharged from the remaining two-thirds of the industry’s vessel capacity, the problem would grow.

It is for this reason that the World Shipping Council and the liner shipping industry continue to support development of a more robust and reliable pre-vessel loading cargo screening capacity, including:

1. Customs’ obtaining more complete shipment data from cargo interests before vessel loading to be used in the container security screening and targeting process. The carrier’s bill of lading data provided to Customs under the 24 Hour Rule is an important component of effective targeting, but no critical examination finds it to be adequate by itself, and
2. Close examination of the feasibility and merits of implementing an advanced overseas container inspection system and strategy, which uses gamma-ray non-intrusive inspection technology and radiation scanning technology on containers before vessel loading.

4. Container Seals and CSDs: No proposed rulemaking has emerged from the Department of Homeland Security regarding container seal verification or “smart box” devices. Initially, both government officials and industry thought that a seal verification rule might be a valuable container security tool. After extensive analysis, however, this is an idea which sounds initially attractive, but in fact would probably provide marginal, if any, security protection in either the prevention or detection of a terrorist risk in a container. It would be difficult and expensive to implement, yet would not help answer the important and most relevant question: What is in the container?

Some of the reasons why DHS officials have expressed substantial reservations about the value or desirability of such a rulemaking include the following.

First, a container seal verification requirement could not be realistically implemented without the deployment of technology on a global scale. In order to prepare for the possibility of a U.S. regulation on this issue, the Council and its member shipping

lines have been working to help develop standards at the International Standards Organization for RFID container seal technology for over two years. We expect that a standard should be approved by the end of this year, and will succeed in being a non-proprietary standard using two radio frequencies. However, the necessary reading infrastructure for RFID container technology requires a global infrastructure of thousands of readers placed at transportation choke points and ports in many different countries around the world. That would be a huge challenge for an infrastructure controlled by thousands of unrelated parties. The deployment of RFID container technology, dependent on fixed readers at thousands of locations around the world, faces real challenges.

Developers of satellite based CSDs fully understand that point and hope to develop a product that can overcome these problems. That kind of container technology, in contrast to RFID which is tied to the problem of fixed readers, may also be able to establish commercial supply chain management benefits with respect to container tracking and *real time* event notification. Such technology, however, has not yet proven to be commercially available at an affordable price.

Second, even if one were to succeed in building such a global RFID container device reading infrastructure, what would it tell you? Somebody opened the container door. This happens thousands of times a year, usually by customs authorities, and every one of these anomalies would require the container shipment to be stopped while an investigation addressed the issue. This fact, plus the uncertain number of false alarms that such devices may generate, would cause many containers to be stopped for an undetermined time. That would probably be acceptable if the result were an assurance the container had nothing bad in it. But that would not likely be the result from such technology.

While it is conceivable that al Qaeda would decide to intercept a container shipment already in transit and insert what it intended to ship inside in the hope that it would not be detected, most security experts think that, if terrorists were to use a container, they would be involved in the container stuffing origin of the shipment, and almost certainly affix appropriate container seals or devices to the container.

Third, contrary to many container device marketing efforts, such devices have not been shown to have significant supply chain management benefits to commercial shippers. Furthermore, a number of the technology vendors interested in such products apparently can only find a profit if they capture the devices' readings in a proprietary data network that they control and resell – a proposition that has clearly received little interest or support from container owners or from their customers.

Any proposal for container seal verification or for application of container security devices warrants a much more detailed dialogue with carriers and shippers than has occurred to date, and a clear demonstration by the government that the effort is a security priority worth the effort.

While the merits and shortcomings of container seals and CSDs can and will continue to be debated, there is no question that CBP's focus on the two ambitious strategies discussed earlier – better shipment data for better container targeting capability, and more complete inspection and scanning of containers – is a prudent and well considered ordering of priorities, which have a far better chance of providing anti-terrorist protection than devices attached to boxes that can't tell you "What's in the box?"

II. European Developments

The European Council of Ministers last year approved a regulation for the Community-wide application of advance ocean container security screening and of Authorized Economic Operator (AEO) programs for both security and trade facilitation purposes. These programs would be analogous, but not identical, to the "24 Hour Rule" and C-TPAT programs in the U.S. Since then, the European Commission has been working to develop regulations that the 25 EU member states would be required to implement regarding these matters.

The most recent draft of the implementing regulation (Commission Regulation 1250), which has been the subject of extensive discussion with the EU member states and with industry, would become effective on July 1, 2009. The AEO program would become effective in all EU Member States on July 1, 2007.

The European Union's basic strategy appears to be properly focused on building advance containerized cargo screening or risk assessment capabilities that can be applied 24 hours before vessel loading, and on improving importers' supply chain security through voluntary AEO programs.

It is unfortunate, therefore, that the European Commission's most recent draft of these regulations has chosen an approach for the implementation of that strategy that contains a fundamental flaw and will not meet the stated objective of effectively enhancing the EU's cargo risk assessment capabilities.

The most significant problem with the pending draft of Regulation 1250 is that it includes a conscious decision to *not* require freight forwarders (NVOCCs under U.S. regulations)¹ to file advance summary declarations (or manifest information) for the shipments they control under their own bills of lading. Only ocean carriers would be required to file pre-vessel loading summary declarations to European national Customs administrations for containerized cargo risk assessment purposes under this 24 Hour Rule.

¹ In the United States, a freight forwarder that issues a bill of lading for the carriage of goods is defined as a "non-vessel operating common carrier" or NVOCC, whereas in Europe they are simply called freight forwarders regardless of whether they undertake the carrier obligations arising from their issuing a bill of lading.

The EU governments' cargo risk assessment system would thus have no meaningful visibility into forwarder controlled shipments, making the entire container security screening effort and the associated costs for ocean carriers and national Customs administrations an empty exercise from a security perspective.

Under the present draft, European customs authorities would get the appropriate advance manifest information from ocean carriers for their shipments, but they would have no insight into those containers controlled by freight forwarders. Advance risk assessment for those forwarder controlled shipments -- which can constitute the majority of the shipments on some voyages -- would thus be based only on knowing, from the ocean carrier's information filings, that a particular freight forwarder was controlling the carriage of various goods from Port A to Port B for undisclosed parties to undisclosed parties. There would be no insight into who the underlying shippers or consignees of the goods really are, or the origins or destinations of the goods.

In taking this approach in the current draft regulations, the Commission has to date rejected the industry proposals that the WSC submitted, jointly with the European Community Shipowners Association (ECSA), the European Shippers Council (ESC), the European freight forwarders (FFI), the international aviation industry (IATA) and the international road transport industry (IRU).

The industry's recommendation has been that freight forwarders should be obligated to file advance pre-vessel loading summary declarations for the shipments they control, just as ocean carriers are obligated to do. This would be in conformance with international practice and with the guidelines approved -- with the European Commission's support -- by the World Customs Organization (WCO), and consistent with advance cargo security screening logic. This approach has been implemented and demonstrated to work satisfactorily under the U.S. and the Canadian 24 Hour Rules.

The Commission has not provided any security-based reasons for rejecting the joint industry filing proposals, other than forwarder filing would make things more complicated and involve more data. This, however, is not very convincing. Customs authorities are responsible for reviewing and processing customs entry of thousands of shipments on every arriving vessel. It hardly seems plausible that these same authorities could not establish an automated system that could accommodate the filing of freight forwarders' summary declarations.

While, as discussed earlier, it is debatable how effective a cargo risk assessment system that solely relies on bill of lading information can be, it is unarguable that a system that excludes bill of lading information for shipments controlled by freight forwarder/NVOCCs would be wholly inadequate and ineffective as a security risk assessment tool.

Without a filing obligation by freight forwarder/NVOCCs, any shipper could easily avoid advance screening of its shipment, (e.g. the underlying shipper and consignee, and the origin and destination of the shipment) by simply contracting for transportation

services with a forwarder instead of an ocean carrier. The resulting illogic is particularly pronounced in European containerized trades that historically have had a significant share of freight forwarder controlled shipments. Without forwarder/NVOCC shipment information, Customs administrations would, for their cargo risk assessments, only be able to review the ocean carrier's bill of lading information. This is likely to show the freight forwarder as both the shipper and consignee, show the foreign load port as the origin and the Community port of unloading as the destination, and oftentimes will only include a general cargo description. This would be insufficient and misleading for cargo risk assessment purposes.

It is too soon to know if the Commission's current draft regulation will be adopted. There is still the hope that the Commission will take the logical step that other nations' 24 Hour Rule regulations have taken, and require freight forwarders to file their shipment data.

While ocean carriers could physically comply with a regulatory requirement that doesn't include forwarder filings, it is apparent that all commercial parties, as well as the various European Customs authorities, would be better off by not implementing a system that has such a significant security flaw.

If governments want to build meaningful pre-vessel loading security screening systems, that is an objective that the liner shipping industry can support. But all appropriate parties should play a proper role in such a system.

III. Some Concluding Thoughts

Whether we like it or not, we live in a world where 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. And, as very recent developments have demonstrated, there is no reason to believe that the threat is going away soon.

The industry fully understands this and has cooperated with national governments and international organizations trying to construct meaningful security regimes. Industry will always be concerned that these measures not unduly delay or restrict commerce or impose costs that produce little added security; however, it will 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. It is not well suited to simplistic formulations or vague "slogan" solutions that aren't supported by clear and specific means to achieve them.

One must also guard against "security fatigue", which can result from trying to digest the mountains of security product promotions, security speeches and presentations, and array of proposals that emerge from so many different sources.

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" strategy, the C-TPAT/AEO concept – 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.

The World Customs Organization has developed international supply chain security standards; however, for various reasons, these are very high level, voluntary guidelines, that will need to be complemented by individual requirements by those nations that decide to undertake their own supply chain security programs. As a result, widespread mutual recognition of AEO programs is unlikely.

The IMO is considering following up on the WCO efforts by trying to determine how the WCO Framework might relate to possible amendment of various IMO conventions. As of now, however, no clear or coherent set of proposals has emerged for how or why WCO Guidelines could or should be converted into IMO convention amendments.

If we are to avoid drifting unproductively in addressing these issues, and if we are to make true progress in enhancing maritime and supply chain security, progress is far 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.

At the same time, industry has a responsibility to support well designed security enhancements.

Global containerized shipping is, in much of the public's mind, dominated by very large importers who generate little public sympathy, and by foreign business enterprises, which can be the subject of political fear-mongering, as the Dubai World Ports debacle so vividly demonstrated. The industry's vulnerability is exacerbated by the fact that, as with most business-to-business enterprises that don't directly touch consumers, most people have no appreciation of the role, importance or magnitude of international trade to their lives and their livelihoods.

The best defense against such risks is to help and support the creation and improvement of a well-conceived, effective, and workable security regime.

The current efforts of CBP and DHS with respect to maritime and supply chain security improvement are certainly worth the industry's support. All sectors of the industry have a reason to work closely and cooperatively with them as they try to define the best way to implement their proposed security strategy improvements.