



WORLD SHIPPING COUNCIL
PARTNERS IN AMERICA'S TRADE

Remarks of

Christopher Koch

President & CEO of the

World Shipping Council

Before the

**Maritime Trades Department, AFL-CIO
2005 Convention**

Chicago

July 22, 2005

I would like to begin this morning by thanking the Maritime Trades Department for the invitation to be here today to discuss maritime security issues. Before addressing that issue, I would like to note with appreciation the excellent efforts of the MTD and its members in consistently contributing to the advancement of the U.S. maritime industry and in supporting the outstanding work of U.S. merchant mariners and other maritime workers. Admiral Brewer of the Military Sealift Command has already addressed the industry's importance in supplying the American armed forces around the world. I'd like to start today by discussing the importance of a healthy and secure maritime industry to the American economy and to individual Americans.

In 2004, Americans imported 10 million loaded cargo containers into the United States. The liner shipping industry transports on average about \$1.5 billion worth of containerized goods through U.S. ports each day. In 2005, a projected 11% growth rate means that the industry will handle more than 11 million U.S. import container loads. In 2006, containerized trade growth is forecasted to increase another ten percent, and we

will need to be ready to handle more than twelve million import containers. And these trade growth trends are not expected to stop after 2006.

Consider the requirements of one customer of our industry. Wal-Mart will import roughly 360,000 FEUs (forty foot containers) this year. If you were to place that volume on trucks bumper-to-bumper in a single line, it would stretch 3,750 miles. And those volumes have to be moved efficiently at the same time as those of L.L. Bean, Target, Home Depot, Ford, K Mart, McDonald's, Hewlett Packard, General Motors, Nike, Becks Beer, Joe's Hardware Store, and thousands of other shippers. And although American international trade is not balanced, it is not just import trades that produce large volumes and trade growth. The top 100 American exporters shipped roughly 2.7 million TEUs of cargo in 2004, including enterprises such as Weyerhaeuser, DuPont, Procter & Gamble, General Electric, Goodyear, 3M, Colgate-Palmolive, and Whirlpool.

And these figures are just for liner shipping. Bulk carriers, tankers, car carriers, LNG vessels, passenger vessels, tug and barge operators all play major roles in supporting the American economy as well.

The demands on all parties in the transportation sector to handle these volumes of commerce efficiently is both a major challenge and very important to the American economy and American consumers.

The maritime industry is faced with dealing with the consequences of two of the more profound dynamics affecting the world today. One is the internationalization of the world's economy and the remarkable growth of global trade – a demand that fills our ships, our ports, and our inland transportation infrastructure, and a demand that will increasingly test our ability to move the large volumes of commerce as efficiently as we have in the past.

The other dynamic is the threat that international terrorism poses to the free flow of international trade, and governments' efforts to respond to that threat. Enhancing maritime security is an unfinished task, with intermodal containerized cargo being a particularly challenging area to address in a way that doesn't unreasonably hamper commerce.

There are many pieces in this effort – ensuring vessel security, port facility security, personnel security, and cargo security.

The Department of Homeland Security (DHS) has stated that there are no known credible threats that indicate terrorists are planning to infiltrate or attack the United States via maritime shipping. At the same time, America's supply chains extend to tens of thousands of different points around the world, and the potential vulnerability of the transportation system requires the development and implementation of prudent security measures. Like many parts of our society, we thus confront an unknown threat, but a known vulnerability.

What is the appropriate collection of measures to address this challenge?

DHS Reorganization

Let's start by noting that Michael Chertoff, the Secretary of the Department of Homeland Security, announced last week a number of initiatives that have emerged from the Department's "Second Stage Review" -- a study of the Department's programs, policies, operations and structure. He has proposed bringing greater organizational clarity and management responsibility to the Department through a number of initiatives, including centralized policy development and coordination, led by an Under Secretary for Policy, and strengthening intelligence functions and information sharing through a new Office of Intelligence and Analysis. The Secretary faces enormous challenges, including, in the maritime transportation sector, creating a truly coordinated security incident prevention and incident response capability. I am confident that we will all work to support his efforts to the best of our abilities.

The Department's *maritime* security efforts involve a number of different, but complementary, pieces, which I will touch on briefly this morning. In providing these comments today, however, it is important to note that the Department is expected soon to produce a National Maritime Security Strategy. This new maritime security strategy, which is expected to be announced later this summer or in the fall, may provide important new direction to a number of the component pieces of the current efforts.

Vessel Security

One of the first missions undertaken after September 11, under Coast Guard leadership, was to address vessel security needs. Today, every arriving vessel above 100 gross tons must have an approved and enforced *vessel security* plan pursuant to the International Ship & Port Facility Security Code (ISPS Code) and Maritime Transportation Security Act (MTSA).

In 2004, a total of 7,241 individual vessels, registered in 81 different countries, made 72,178 U.S. port calls. In the first month of enforcement of this new security regime, the Coast Guard found that 2.5 percent of vessels arriving in U.S. ports were significantly non-compliant with the new security requirements, and they were denied entry to port, detained in port, or expelled from port as a result. By the end of December 2004, the percent of vessels arriving in U.S. ports with major problems fell to 1.5 percent.

The Coast Guard is also targeting vessels for increased inspections if they are registered in a country whose vessels have below average compliance in meeting safety or security requirements, and it is making those registries public.

In short, through a combination of continued effective flag state and port state enforcement efforts and industry attention to vessel security plan compliance, ship

security enhancement is proceeding well. Those that are not undertaking adequate compliance efforts are being identified and their vessels are being detained.

The Coast Guard has reason to feel proud of how it was able to help create and implement this new vessel security regime. The agency would be the first to say, however, that it has many challenges to address. One of the Coast Guard's more difficult challenges is trying to ensure that smaller vessels operating in our waters -- those less than 100 tons that are not covered by the ISPS Code -- are secure. Patrolling the thousands of square miles of U.S. waters to deter the possibility of sabotage, small vessel attack such as the attacks on the *U.S.S. Cole* or the *Limburgh*, or other possible security incidents, is an immense challenge.

Port Facility Security

The ISPS Code, which governs ship security plans, also requires the establishment of *port facility security* plans. All major U.S. port facilities now have security plans approved by the Coast Guard. The governments of our trading partners are implementing the Code at their ports. As I noted earlier, the Coast Guard can and does use its "port state" enforcement authority to ensure that all vessels, including those under foreign registries, are complying with the Code. This "port state" control mechanism doesn't apply to facilities in other jurisdictions. Consequently, in order to monitor and reinforce the need for effective and compliant security plans at foreign ports, the Coast Guard has established the International Port Security Program, pursuant to which the agency visits foreign ports and terminals around the world to share and align security practices and assess compliance with the ISPS Code. The industry has a strong interest in working with the Coast Guard to ensure that all port facilities around the world are ISPS Code compliant.

Personnel Security

A third part of the DHS security strategy is to try to ensure that the people working in the maritime transportation system meet appropriate security criteria. This involves a number of different types of workers.

U.S. Domestic Transportation Workers: The Maritime Transportation Security Act requires the Department of Homeland Security to establish a Transportation Worker Identification Credential (TWIC). DHS would issue a TWIC, after criminal and security background checks, as a minimum baseline document to those persons who need unescorted access within a secure maritime facility in the U.S., such as truck drivers or dock workers. The TWIC should be valid for use nationwide, so that truck drivers, longshoremen and others don't need multiple security credentials for every port facility they may work at. Notwithstanding the efforts of the Coast Guard to push for the implementation of the TWIC, it appears that DHS will not issue a proposed rulemaking on this issue until sometime in 2006 at the earliest. While this is an admittedly ambitious

and difficult initiative, the need for a uniform federal credentialing document is well established, and the lack of more expeditious progress on this issue is unfortunate.

U.S. Merchant Mariners: U.S. seafarers already go through a Coast Guard vetting process when obtaining their merchant marine documents (MMD), and the Coast Guard has been working over that past couple of years to improve this process. It is not clear the exact relationship of the TWIC and the MMD, although it is clear that the Coast Guard wants to create a single document that seafarers could be issued that would meet both TWIC and MMD requirements.

The National Maritime Security Advisory Committee, which I am privileged to chair, was recently asked by DHS for its views on a number of issues relating to the development of the TWIC. The Committee's recommendations were greatly assisted by the input of Committee members Bill Eglington of the Seafarers International Union and Jim Stolpinski of the International Longshoremen's Association.

Foreign Seafarers: Foreign seafarers have faced a different kind of challenge, and many of you here today work with the International Transport Workers Federation in an effort to ensure fair treatment of foreign seafarers. After September 11, the government established the requirement that all foreign seafarers must have individual visas if they are to get off a ship in the U.S. The individual visa application and processing procedures provide the requisite security check. This is an understandable policy, but it has also produced some difficulties that seafarer rights organizations and others have identified. Seafarers without individual visas cannot obtain shore leave privileges while in U.S. ports, and this is a hardship on those individuals. Furthermore, non-visa seafarers, if from a list of 26 specified nations, can cause the government to require armed guards on the vessel -- a policy that remains controversial in so far as armed guards are concerned.

It is difficult to see a change in the government's visa policy in the foreseeable future. The Coast Guard has expressed some interest in whether foreign seafarers arriving on ships to the United States should also hold a Seafarer Identity Document that meets the revised requirements of the 2003 ILO Seafarers' Identity Documents Convention, which entered into force for ratifying countries (currently four) on February 9th. There are a number of unresolved questions with respect to this idea, however, because: 1) the U.S. government has indicated it will not seek ratification of the ILO Convention; 2) the U.S. government has not yet identified a clear role for the ILO documents for foreign seafarers, as individual visas will continue to be required for entry and shore leave; 3) the ILO documents would be issued by each seafarer's country of domicile (and it is not clear that the U.S. would accept all such documents at face value or as providing assurances as to the seafarer's exact identity); and 4) the biometric identifiers in the ILO document have been determined by DHS as not meeting the requirements for biometric identifiers that today are being collected under the U.S. government's U.S. VISIT program.

Cargo Security or “Supply Chain” Security

Developing and implementing measures that produce reliable security measures for ships, port facilities, and maritime and port transportation workers is a complex challenge. But they are not as complicated as the challenge of developing an effective and reliable *cargo security* regime, especially intermodal, containerized cargo. There are several elements and programs that comprise the government’s cargo security strategy, and each has a role, including:

- The C-TPAT Program and the Container Security Initiative
- Enhancing In-Transit Container Security
- Cargo Security Risk Assessment Screening
- Technology and Security Enhancement.

1. C-TPAT and CSI

Customs’ Trade Partnership Against Terrorism (C-TPAT) is an initiative intended to increase supply chain security through voluntary, non-regulatory agreements with various industry sectors. Its primary focus is on the participation of U.S. importers, who are in turn urged to have their suppliers implement security measures all the way down their supply chains to the origin of the goods. This approach has an obvious attraction in the fact that the importer’s suppliers in foreign countries are beyond the reach of U.S. regulatory jurisdiction. In return for participating in the program, importers are given a benefit of reduced cargo inspection. The C-TPAT program invites participation from other parties involved in the supply chain as well, including carriers, customs brokers, freight forwarders, U.S. port facilities, and a limited application to foreign manufacturers.

C-TPAT has improved the security of importers’ supply chains, yet it remains a program that faces criticism and an unclear future. C-TPAT should be understood for what it is and what it is not. C-TPAT is a set of voluntary partnerships between CBP and willing industry members. C-TPAT is not a regulatory program. It should not be confused as being one. Nor should it be a substitute for regulations when the government has clear, specific things it wants industry to do to enhance security. The difficulty is that the program is in some respects ambiguous, and perhaps unavoidably so.

Ocean carriers receive no direct benefits from CBP for participation in the program, but have nevertheless joined this “voluntary partnership” program with CBP. C-TPAT is an evolving initiative, and industry and government will learn and adapt as it matures. For example, when the Sea Carrier portion of C-TPAT was originally formulated, there were no ISPS Code, no Coast Guard MTSA regulations regarding vessel and port facility security plans, and no requirement for automated electronic filing of cargo manifests, so C-TPAT carriers recognized the regulatory void and agreed to undertake a number of voluntary measures in this regard. Today, there are comprehensive regulations on these issues.

Ocean carriers are working with CBP officials to determine how the next phase of the C-TPAT program for carriers will evolve, and they wish to continue to work with CBP and other DHS agencies to determine appropriate ways to supplement the regulatory security regime.

At the same time, Customs recognizes that no nation and no single program by itself can protect international trade. International cooperation is essential. For ships and port facilities, the International Maritime Organization (IMO), a U.N. regulatory agency with international requirement setting authority, has responded to U.S. leadership and created the International Ship and Port Security Code (ISPS). These IMO rules are internationally applicable and are strictly enforced by the U.S. Coast Guard. There is, however, no comparable international regulatory institution with rule writing authority for international supply chain security.

At the World Customs Organization, CBP has worked diligently with other governments on a supply chain security framework that can be used by all trading nations. This framework will be useful, but it is at a fairly high policy level and will be implemented on a voluntary basis by interested governments. Consequently, U.S. and foreign customs authorities must also create a network of bilateral cooperative relationships to share information and to enhance trade security.

This is the Container Security Initiative. The Council supports this program and the strategy behind it. Today more than 60% of U.S. containerized imports pass through operational CSI ports, with further program growth expected. The liner shipping industry is fully supportive of these efforts by Customs authorities and hopes the program will continue to expand as expeditiously as possible.

2. Enhancing In-Transit Container Security

While the most important and challenging container security issue is ensuring that containers are securely loaded with cargo in the first place, it is also important to have a system that can help determine whether a container may have been tampered with while in-transit. In this regard, CBP and DHS are currently in the process of drafting proposed regulations that would require a verification of container seals on inbound containers before they are loaded aboard vessels bound for the U.S. We expect this rule to be proposed for public comment by late summer or fall. This will be a costly and challenging rule for the industry and CBP to implement, but we recognize the need to address this issue and the need for a container seal verification rulemaking.

Some of the more important issues that will need to be addressed in this rulemaking will be: the reporting process to CBP when a seal anomaly is identified, the consequences to the shipment when a seal anomaly is identified, where the seal verification is to take place, and a reasonable implementation time frame that will allow port facilities around the world to develop implementation measures.

3. Cargo Security Risk Assessment and the National Targeting Center

The stated and statutorily mandated strategy of the U.S. government is to conduct a security screening of containerized cargo shipments *before* they are loaded on a U.S. bound vessel in a foreign port. The World Shipping Council fully supports this strategy. The correct time and place for the cargo security screening is before the containers are loaded on a ship. We know that America's seafarers agree. Most cargo interests also appreciate the importance of this strategy, because they don't want their shipments aboard a vessel delayed because of a security concern that could arise regarding another cargo shipment aboard the ship.

In order to be able to perform this advance security screening, Customs and Border Protection implemented the "24 Hour Rule" in early 2003. Under this rule, ocean carriers are required to provide Customs with their cargo manifest information regarding all containerized cargo shipments at least 24 hours before those containers are loaded onto the vessel in a foreign port. The Council supports this rule. Customs, at its National Targeting Center in Northern Virginia, then screens every shipment using its Automated Targeting System (ATS), which also uses various sources of intelligence information, to determine which containers should not be loaded aboard the vessel at the foreign port, which containers need to be inspected at either the foreign port or the U.S. discharge port, and which containers are considered low-risk and able to be transported expeditiously and without further review. Every container shipment loaded on a vessel for the U.S. is screened through this system before vessel loading at the foreign load port.

The Department of Homeland Security's strategy is thus based on its performance of a security *screening* of relevant cargo shipment data for 100% of all containerized cargo shipments before vessel loading, and subsequent *inspections* of 100% of those containers that raise security issues after initial screening. Today, we understand that CBP inspects roughly 5.5-6% of all inbound containers (over 500,000 containers/year), using either X-ray or gamma ray technology (or both) or by physical devanning of the container.

We all have a strong interest in the government performing as effective a security screening as possible before vessel loading. Experience also shows that substantial disruptions to commerce can be avoided if security questions relating to a cargo shipment have been addressed prior to a vessel being loaded and sailing. Not only is credible advance cargo security screening necessary to the effort to prevent a cargo security incident, but it is necessary for any reasonable contingency planning or security incident recovery strategy.

Today, while the ATS uses various sources of data, the only data that the commercial sector is required to provide to Customs for each shipment for security screening is the ocean carrier's bill of lading/manifest data filed under the 24 Hour Rule. This was a good start, but carriers' manifest data has clear limitations.

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 ATS by the U.S. importer or the foreign exporter that can be used in the pre-vessel loading*

security screening process, even though these parties possess shipment data that 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"¹. Today, cargo entry data is required to be filed with CBP by the importer, *but* is not required to be filed until after the cargo shipment is in the United States, often at its inland destination – too late to be used for security screening purposes.

Last fall, the COAC² Maritime Transportation Security Act Advisory Subcommittee submitted to DHS a recommendation that importers should provide Customs with the following data before vessel loading:

1. Better cargo description (carriers' manifest data is not always specific or precise)
2. Party that is selling the goods to the importer
3. Party that is purchasing the goods
4. Point of origin of the goods
5. Country from which the goods are exported
6. Ultimate consignee
7. Exporter representative
8. Name of broker (would seem relevant for security check.)
9. Origin of container shipment – the name and address of the business where the container was stuffed.

The Council agreed with this recommendation. The government's strategy today is to inspect containerized cargo on a risk-assessment basis. An ocean carrier's bill of lading by itself is not sufficient for effective cargo security screening. Accordingly, the government should improve the cargo shipment data it currently uses for its risk assessment.

The part of DHS Secretary Chertoff's speech last week that touched directly on maritime commerce was his explicit recognition that the government's current container/supply chain security risk assessment system must be improved and that the government needs to obtain additional advance cargo shipment information before vessel loading to perform more meaningful and effective security risk assessment. Implicit in his speech was the fact that this information must be obtained from the cargo interests shipping the goods. He stated:

"I believe that we can gather, fuse and assess more complete data from the global supply chain to develop a more accurate profile of the history of cargo in a given container. Data about what cargo is moving from the initial point of shipping to the final destination will allow us to target risk better. With more informed targeting, we can more efficiently conduct inspections of cargo that

¹ 46 U.S.C section 70116(b)(1). Section 343(a) of the Trade Act also requires that cargo information be provided by the party with the most direct knowledge of the information.

² The Departmental Advisory Committee on Commercial Operations of Customs and Border Protection or COAC is a twenty member advisory committee to the Departments of Homeland Security and Treasury.

is either high risk or unverified. This “Secure Freight” initiative will allow us to expedite large portions of the inbound that sustains our nation’s economy, and focus with more precision on the unknown.”

While it is too early to know what specifically DHS has in mind in creating this “Secure Freight” Initiative, or how it may relate to current Customs systems and capabilities, the Secretary was clearly correct in identifying this issue as one deserving the Department’s priority attention. It is important for two reasons. First, by having a more complete and accurate picture of what cargo is being bought and sold, by whom, and from where, the government can improve its capability to prevent illegal acts, including terrorist attacks. Second, by having this more complete information, the government will have a faster and better capability to analyze any security incident that does occur and better information and capability to restore the flow of commerce in the wake of an incident. One might reasonably expect that the National Maritime Security Strategy, when it is announced later this year, will include more details on the Secure Freight Initiative.

4. Technology and Security Enhancement.

Technology clearly has a role in increasing the efficiency and security of containerized cargo shipments. This morning I would like to briefly touch on three areas where technology is being explored: RFID technology, the “smart box” concept, and container inspection technology.

RFID Technology: In anticipation of the U.S. government’s expected promulgation of regulations requiring the verification of container seals, considerable effort has been expended by ocean carriers and technology vendors to develop standards for electronic RFID (radio frequency identification) seals, container tags, and shipment tags.

RFID container tags (that provide the “license plate” information about a container) and shipment tags (that provide a shipper with the option of inputting details about their cargo shipment) would have little, if any, bearing on container or supply chain security. These would be products that would be used only if they provided sufficient equipment management or supply chain management benefits to warrant the investment – a prospect that appears questionable at least for the near future.

Electronic RFID seals, or “e-seals”, however, could provide an automated, more effective and more efficient way to verify container seals, and thus there is considerable industry interest in them. One of the present challenges, however, is to develop an agreed technology standard for such devices. This is a complicated issue, made more complicated by technology vendors competing visions of the appropriate issues and solutions, but we remain hopeful that by the end of this year that an e-seal standard can be developed.

“Smart” Box: In addition to these developments, there is a discussion within the government of “smart” containers, a term that frequently means a container that has a “container security device” or “CSD” attached. There are presently more questions than answers on this topic, including:

- What specifically would make a container “smart”? Present thinking in Customs involves a device that would sense if the right-side container door has been opened.
- What the appropriate technologies may be for such an objective.
- Whether they would “work”, what the reliability and accuracy of the devices would be, and what their impact on operations would be.
- Developing an international standard for such a device – a process that has not been started.
- Who would read the devices, and how would that party know which boxes have CSDs to be read? Where would they be read?
- Who would build and operate the reading infrastructure? What would be done with the information, and how would exception reporting be handled?

At the same time, there is also discussion within DHS of a “next generation” or “Advanced CSD” with more sophisticated sensors that DHS is researching, which will also need to address a similar set of issues, including what specifically is it that needs to be “sensed”, the accuracy and reliability of the device, its cost, who applies the device, the reading infrastructure that would be needed, who would read it, when and where, and the protocols for how different readings would be addressed by whom and when.

The idea of transforming containers into “smart”, impregnable fortresses clearly has an appeal. Reality, however, requires addressing issues of: technology definition and standards; false positives from sensor technologies and their consequences; questions about device reliability; maintenance complexity; device failures and equipment out of service time; power needs and failures, including battery life issues; device costs; and labor issues and costs.

In addition, technology can bring new security vulnerabilities that have to be considered. For example, permanent or reusable container security technology devices would require a capability to “write” new information into the device or amend existing information in the device. Such a capability would require a wide range of parties around the world to be given the capability of writing new information into container security devices, which would create troubling security vulnerabilities of third parties becoming capable of “hacking” into the devices. It is for this very reason that the international electronic seal standard being developed will require that e-seals be one-time use seals without the capability to write or change the information in the seal.

In short, this is a very complex and technically challenging subject and one that is receiving considerable attention by the maritime industry, technology vendors, and government officials. It would appear that in the area of container affixed security technologies, RFID e-seals are likely to be the devices with the most likely chance of seeing application in the near future.

Container Inspection Technology:

Today, X-ray and gamma ray non-intrusive container inspection equipment (NII) is being deployed at U.S. and foreign ports to facilitate the inspection of containers. The use of the technology has generally required delaying the inspected box and disrupting its scheduled handling at the port, but it is generally recognized as an appropriate way to check a container about which there are significant security questions.

A particular security concern is the potential use of a container to transport a nuclear or radiological device. While there is no evidence that terrorists have nuclear weapons or devices, or that a shipping container would be a likely means to deliver such a device, the consequences of the potential threat – including those from a low tech “dirty bomb”-- are sufficiently great that, CBP is deploying radiation scanning equipment at all major U.S container ports, with the objective of being able to check every container entering the U.S. for radiation by the end of this year. CBP and the Department of Energy are also working with foreign ports to encourage the installation of radiation scanning technology abroad as well.

It is in the area of container inspection technology improvement, however, that some of the more significant changes to the present supply chain security regime may be evolving.

As an objective, any and all containers that present a security issue should be inspected before the container is loaded aboard ship. Today, the expense, difficulty and delays of conducting container inspections, plus the process of obtaining the necessary cooperation and inspection of the container by the foreign customs authority, has made such an objective impractical, except in the cases of containers of high concern.

There is reason to believe that container inspection technology may be evolving to the point that it could be deployed in the foreseeable future to allow radiation and NII inspection of all containers entering a port facility without significant delay to commerce. If this were to prove true, and if the radiation and image readings are of sufficient quality for security screening purposes, this capability would allow a new and significantly more effective supply chain security strategy to be deployed. Such capability could enable DHS and other governments to “flex” their security screening capabilities, to inspect more containers, even from a remote location, without having to inconvenience terminal operators or other customs authorities, and to more effectively handle a response to a transportation security initiative, including the NII inspection of every container being loaded at a particular port, if needed.

More importantly, this technology, unlike so many others, helps address the security question of paramount importance – namely, what’s in the container?

We understand that DHS officials are presently reviewing the threshold question, which is “does the technology work”? Included in this process is a review of tests being conducted at two different Hong Kong port facilities of radiation-NII inspection of the containers entering those facilities. The evaluation of the technology is the first step.

If the technology works, the next step should be to determine how the information produced by this technology would be used. That will be more complicated, but would also seem achievable. The technology obviously must be physically sited on marine terminals around the world. This would be a challenge, but not beyond reasonable expectation, providing the correct incentives are established -- one of which would be a clear U.S. government desire to obtain such a capability. More challenging is to determine how the technology's readings and images would be used and analyzed, by whom and when. This will require addressing roles and responsibilities, and issues of liability (terminal operators are unlikely to accept the liability of making security judgments based on the readings). This would presumably require operational integration with CBP's National Targeting Center, and a more proactive interest in and capability of calling up and reviewing container images before vessel loading.

While there are real and legitimate issues that need to be addressed in considering this technology and its possible deployment, the capability for governments to call up and review radiation and NII images of any container before vessel loading without delaying commerce could provide a quantum improvement in security capabilities. In fact, if it works, it could allow governments the flexibility to change their strategies in a way that would provide increased security assurance for all legitimate commerce.

Summary

When addressing the issue of international supply chain security, we find ourselves dealing with the consequences of two of the more profound dynamics affecting the world today. One is the globalization of the world economy, the remarkable growth of world trade, and the U.S. economy's appetite for imports -- a demand that fills our ships, our ports, and our inland transportation infrastructure, and a demand that will increasingly test our ability to move America's commerce as efficiently as we have in the past.

The other dynamic is the threat to our way of life from terrorists and the challenge of addressing the vulnerabilities that exist in the free flow of international trade, even when the specific risk is elusive or impossible to identify.

Finding the correct, reasonable balance between prudent security measures and overreacting in a way that impairs commerce is a tough challenge.

We are making real progress in addressing these challenges, but that the effort to address them more effectively must continue.

I am pleased to be here today because I believe that the maritime industry and the maritime labor community are very much on the same page when it comes to enhancing maritime security. We have both supported enhancing ship security. We have both

supported enhancing port security. We have both supported enhancing personnel security, while respecting the rights of the individual.

We both want to see a more effective supply chain security regime so that we can be confident that our ships, our crews and the legitimate cargo aboard our ships are protected.

The World Shipping Council and our member companies believe that there is no task more important than helping government develop effective maritime and cargo security initiatives that do not unduly impair the flow of commerce. We look forward to working with you all on that shared objective.