Testimony of

Christopher Koch
President & CEO of the
World Shipping Council

Regarding

Securing Maritime Commerce and Global Supply Chains

Before the

Permanent Subcommittee on Investigations
of the
Senate Committee on Homeland Security and Governmental Affairs

March 30, 2006

Introduction

Mr. Chairman and members of the Committee, thank you for the opportunity to testify before you today. My name is Christopher Koch. I am President and CEO of the World Shipping Council, a non-profit trade association representing international ocean carriers, established to address public policy issues of interest and importance to the international liner shipping industry. The Council's members include the full spectrum of ocean common carriers, from large global operators to trade-specific niche carriers, offering container, roll-on roll-off, car carrier and other international transportation services. They carry roughly 93% of the United States' imports and exports transported by the international liner shipping industry, or more than $500 billion worth of American foreign commerce per year.[1]

[1] A list of the Council's members can be found on the Council's website at www.worldshipping.org.

I also serve as Chairman of the Department of Homeland Security's National Maritime Security Advisory Committee, as a member of the Departments of Homeland Security's and Treasury's Advisory Committee on Commercial Operations of Customs and Border Protection (COAC), and on the Department of Transportation's Marine Transportation System National Advisory Council. It is a pleasure to be here today.

In 2005, American businesses imported roughly 11 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 2006, at projected trade growth rates, the industry will handle roughly 12 million U.S. import container loads. And these trade growth trends are expected to continue.

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

At the same time that the industry is addressing the issues involved in efficiently moving over 11 million U.S. import containers this year, we also must continue to enhance maritime security, and do so in a way that does not unreasonably hamper commerce.

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 containers. At the same time, America's supply chains extend to tens of thousands of different points around the world, and the potential vulnerability of containerized transportation 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?

The Department of Homeland Security's maritime security strategy involves many different, but complementary, pieces.

It includes the establishment of *vessel security* plans for all arriving vessels pursuant to the International Ship & Port Facility Security Code (ISPS Code) and the Maritime Transportation Security Act (MTSA).

It includes the establishment of U.S. *port facility security* plans and area maritime security plans pursuant to the ISPS Code and MTSA, and the establishment by the Coast Guard of the International Port Security Program (IPSP) pursuant to which the Coast Guard visits foreign ports and terminals to share and align security practices and assess compliance with the ISPS Code.

It includes the Maritime Domain Awareness program, under which DHS acquires enhanced information about vessel movements and deploys various technologies for

better maritime surveillance. The challenge of effectively patrolling all the coasts and waters of the United States is obviously a large one.

The MTSA directives and DHS efforts also include enhanced security for *personnel* working in the maritime area.

And last, but certainly not least, these directives and efforts include an array of initiatives to enhance *cargo security* – the important topic of this hearing, including

- Cargo Security Risk Assessment Screening
- The Container Security Initiative
- The Customs Trade Partnership Against Terrorism (C-TPAT) Program, and
- Container Inspection Technology Deployment.

The liner shipping industry and the World Shipping Council have fully supported these various initiatives. Ocean carriers' business depends upon the government having a security regime that provides adequate levels of security confidence, while continuing to allow for the efficient and reliable transportation of America's exports and imports. I will now turn to the issues the Committee, in its March 13 letter of invitation, requested that my testimony address today.

Committee Question #1: The private sector perspective on U.S. government programs related to maritime and port security.

The government's multi-layer security strategy is a fundamentally sound one, and seeks to address cargo and maritime security on an international basis as early as is practicable. It does not wait to address security questions for the first time when a ship and its cargo arrive at a U.S. port. The strategy can be further developed and strengthened, however, and we appreciate the Committee's continued interest in these issues. The following is a brief description of the strategy's various layers.

A. Vessel Security

Every vessel entering a U.S. port, whether of U.S. or foreign registry, must have a ship security plan that is in accordance with the ISPS Code – a binding international convention developed under the leadership of the U.S. Coast Guard. The Coast Guard also ensures through its port state enforcement programs that vessels entering U.S. ports are in compliance with the Code. Vessels that are not in compliance are denied entry into a U.S. port by the Coast Guard.

Under MTSA, the Coast Guard requires vessels to file Notices of Arrival 96 hours before arrival in a U.S port, providing relevant advance information about the vessel, its itinerary, its crew and its cargo. The Coast Guard and Customs and Border Protection (CBP) use this information for risk profiling.

B. Port Security

Port facilities must also comply with the ISPS Code, and, in the U.S., the Coast Guard's MTSA regulations – the regulatory regime used to implement the ISPS Code domestically. All major U.S. port facilities are in compliance with the ISPS Code.[2]

These port facilities or marine terminals may be operated by the state or local government public port authority, or they may be leased from the port authority by terminal operating service providers, with the port authority maintaining ownership and oversight of the port. The majority of U.S marine terminals are operated by private marine terminal firms, which have leased the property from the port authority. Major ports generally have multiple terminals and terminal operators.

Foreign port facilities must also comply with the ISPS Code, and the U.S. Coast Guard oversees this under its International Port Security Program (IPSP). Coast Guard IPSP officers visit port facilities around the world, and feed the results from each IPS assessment into the agency's port state control security matrix, and work with the local governments if necessary to try to improve conditions if warranted.

As a way to support the Coast Guard's efforts in this regard, the World Shipping Council and Coast Guard last week formalized a voluntary reporting mechanism whereby the Council's companies can assist the Coast Guard's global maritime security efforts by reporting port facility security status issues to the Coast Guard. The intent of this effort is to provide the Coast Guard with additional information that may help the agency better prioritize its IPSP efforts, work with other governments, and enhance domestic enforcement of maritime security requirements.

C. Personnel Security

Maritime personnel security is addressed in various ways. Vessels must provide CBP and the Coast Guard with advance notice of all crew on the vessel 96 hours before the vessel arrives in a U.S port for screening. U.S. seafarers are issued credentials by the U.S. Coast Guard and must go through a security vetting process. All foreign seafarers must have valid, individual U.S. visas if they are to go ashore in the U.S.

Regarding personnel working in U.S. ports, the Department of Homeland Security has indicated that it intends to promulgate proposed rules on the Transportation Worker Identification Credential (TWIC) in the near future, as required by MTSA. At the request of DHS, the National Maritime Security Advisory Committee, after intensive, open and constructive dialogue amongst diverse industry and government officials, approved a detailed set of recommendations to the Department for its consideration in the development of this initiative. The establishment of the TWIC would help meet one of

[2] The Coast Guard's MTSA regulations estimated that the industry's compliance with the Code would cost more than $8 billion over ten years, and that figure did not include foreign port or foreign vessel compliance costs.

the unaddressed U.S. port security imperatives identified by Congress and DHS as an essential element of the nation's maritime security. The Council and its Member lines strongly support DHS promulgating a regulation on this issue. This issue remains one of the most important uncompleted tasks to improve U.S. port security.

D. Cargo Security

Particularly with respect to containerized cargo, the issues surrounding cargo security are challenges that require a multi-faceted strategy, which begins long before the cargo arrives at a U.S. port. It involves advance Customs security screening of all containers before vessel loading in a foreign port, cooperation with foreign Customs authorities through the Container Security Initiative, use of container inspection technology, and the Customs Trade Partnership Against Terrorism initiative.

a. 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 all 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. Most cargo interests also appreciate the importance of this strategy, because they don't want their shipments put at risk or 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, CBP implemented the "24 Hour Rule" in early 2003. Under this rule, carriers are required to provide CBP 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.

CBP, 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 bound for the U.S. is screened through this system before vessel loading at the foreign port. Customs may issue the carrier a "Do Not Load" message on any container that is so screened if it has security concerns that need to be addressed.

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 (roughly 600,000 containers per

year), using either X-ray or gamma ray technology (or both) or by physical devanning of the cargo.

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. Not only is credible advance cargo security screening necessary to the effort to try to prevent a cargo security incident, but it is necessary for any reasonable contingency planning or incident recovery strategy.

Today, while the ATS uses various sources of data, the only data that the commercial sector is required to provide to CBP for each shipment for the before-vessel-loading 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 limitations.

Cargo manifest data should be supplemented in order to provide better security risk assessment capabilities.[3] *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*. This occurs, even though these parties 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".[4] Today, cargo entry data is required to be filed with CBP by the importer, *but* is not required to be filed until <u>after</u> the cargo shipment is in the United States, often at its inland destination – too late to be used for security screening purposes.

In September 2004, the COAC Maritime Transportation Security Act Advisory Subcommittee submitted to DHS a recommendation that importers should provide CBP with the following data elements 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.), and
9. Origin of container shipment – the name and address of the business where the container was stuffed, which is often not available from an ocean carrier's bill of lading.

[3] *See also*, "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection", General Accounting Office Report and Testimony. March 31, 2004 (GAO-04-557T).
[4] 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.

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

If a risk assessment strategy is to remain the core of the government's cargo security system, the government needs to decide what additional advance cargo shipment information it needs to do the job well. It may include the data elements recommended above, or it may include additional desired data elements beyond that list. While this is not a simple task, it is important that progress be made on deciding what additional data should be obtained for this purpose, and it is important that the cargo interests, and not just carriers, be required to provide the relevant data in time to do the advance security screening before vessel loading in the foreign port.

b. Container Security Initiative

No nation by itself can secure or 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 no comparable international regulatory institution with rule writing authority for international supply chain security. For a variety of reasons, the World Customs Organization (WCO) has not acquired such authority.

At the WCO, CBP continues to work with other governments on a supply chain security framework that can be used by all trading nations. This framework may be useful, but remains at a fairly high 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 fully supports this program and the strategy behind it.

Today, 73.5% of U.S. containerized imports passes through 44 operational CSI ports, with further program growth expected. CBP hopes to expand the CSI program to 55 ports, which could cover roughly 85% of U.S containerized imports.

A listing of operational CSI ports follows:

Port Name	TEUs in 2005 (in thousands) US Imports
Yantian (Shenzhen)	2,342.38
Hong Kong	1,866.14
Shanghai	1,696.41
Kaohsiung	1,154.69
Busan	1,121.67
Singapore	534.56
Rotterdam	457.32
Bremerhaven	432.68
Antwerp	317.80
Tokyo	288.77
Nagoya	187.92
Laem Chabang	178.38
Cortes	172.8
Le Spezia	158.42
Hamburg	158.41
Santos	155.70
Salalah (Oman)	129.60
Kobe	129.50
Genoa	122.87
Yokohama	122.74
Le Havre	120.83
Colombo	114.30
Gioia Tauro	96.14
Livorno (Leghorn)	96.02
Felixstowe	73.70
Algeciras	60.35
Buenos Aires	54.88
Liverpool	43.42
Tanjung Pelepas	43.25
Durban	42.26
Port Kelang	40.42
Thamesport	33.36
Naples	33.19
Southampton	32.35
Lisbon	22.90
Halifax	22.86
Gothenburg	19.13
Piraeus	10.18
Vancouver	8.99
Tilbury	2.92
Dubai	0.98
Marseille	0.69
Montreal	0.17
Zeebrugge	0.04
Total CSI Ports	*12,702.09*
Non-CSI Ports	*4,588.26*
Total All Ports	*17,290.35*

c. C-TPAT

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 some Mexican and Canadian manufacturers.

CBP has been working to strengthen the C-TPAT program and to increase validations of participants' performance. C-TPAT is not a regulatory program, and it is not a guarantee of security. It does, however, provide for a creative partnership approach between government and industry as one element of a multi-layered strategy to improve security. It clearly has value, even though it can't be easily measured or quantified; and, because its principal purpose is to try to affect the conduct of parties outside U.S. regulatory jurisdiction, it has a reach that regulations alone could not have.

Many maritime and supply chain security issues can be, should be, and are addressed through regulatory requirements, not C-TPAT. For example, vessel security plans and port security plans are regulated by Coast Guard regulations implementing the ISPS Code and MTSA. The data that must be filed with CBP to facilitate cargo security screening must be addressed through uniformly applied regulations. Seafarer credentials and the Transportation Worker Identification Card must be addressed through uniformly applied requirements.

C-TPAT, however, is a program that can try to address matters that are not or cannot be addressed by regulations, such as supply chain enhancements beyond U.S. regulatory jurisdiction, or matters that aren't covered by regulations.

Committee Question #2: The private sector perspective on foreign ownership of U.S. terminals

Stevedoring and marine terminal operations are a service industry that is open to foreign investment. Billions of dollars of foreign investment has been made in the U.S. over recent years in this sector, and that investment has contributed substantially to a transportation infrastructure that is critical to moving America's commerce efficiently and reliably. The investment has come from Japanese, South Korean, Danish, British, Chinese, French, Taiwanese, and Singaporean businesses, just as American companies

have been allowed to invest in marine terminal and stevedoring businesses in foreign countries.

The substantial majority of American containerized commerce is handled in U.S. ports by marine terminal operators that are subsidiaries or affiliates of foreign enterprises, usually the container shipping lines themselves. This is an international, highly competitive industry, providing hundreds of thousands of American jobs. The United States depends on it, and it in turn has served the needs of American commerce well, adding capacity and service as the needs of American exporters and importers have grown.

An important element of the U.S. government's position in international trade negotiations for many years, under both Democrat and Republican administrations, has been the importance of securing the ability of international investment to flow into various international service industries. It is a principle of substantial importance to many sectors of the American economy. There are many billions of dollars of American service industry investments around the world, including banking, insurance, food service, accounting, construction, energy, engineering, etc.

U.S. marine terminal facilities, whether operated by U.S. or non-U.S. owned companies, must and do comply with all the government's applicable security requirements. There is no evidence that terminal facilities' operations conducted by foreign controlled companies are any less secure, or in any way less compliant with security regulations, or in any way less cooperative with U.S. government security authorities than U.S. controlled companies. In fact, these companies work closely and cooperatively with the Coast Guard, Customs and Border Protection, the U.S. military, and other U.S. law enforcement agencies.

This is an international industry and has been for many years. Less than 3% of American international maritime commerce is transported on U.S.-*flag* ships, and foreign owned carriers are responsible for the capital investment in most of those ships. American *owned* liner shipping companies transport roughly 5% of the trade, and their vessels are largely foreign flag.

The leading American liner shipping companies, such as Sea-Land, APL, and Lykes, were sold by their U.S. owners years ago to foreign companies, and neither the Executive Branch nor an informed Congress did anything to protest or stop this change. Foreign ownership of shipping companies and U.S. marine terminal operating companies has been part of our nation's economic make-up for years. We live in a global economy and society where it is simply a fact that most of this important component of the nation's "critical infrastructure"[5] is owned and operated by foreign companies. One might wish

[5] The liner shipping industry and marine terminal operators logically fall within the most commonly used definitions of "critical infrastructure". *See, e.g.*, the National Infrastructure Protection Plan definition: "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, networks or functions would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The

American companies were dominant industry actors, but they aren't. Further, U.S. financial markets have demonstrated little enthusiasm for international liner shipping due to its high capital investment requirements, cyclicality, and intense competition, as well as the fact that other nations' tax laws are more favorable to shipping.

The U.S. has been well served by the investment capital these foreign companies have made and continue to make in serving U.S. commerce.[6] The United States' economy and U.S. importers and exporters would be significantly harmed by policies that discourage or prevent this foreign investment. This is particularly true now with trade volumes pressing U.S. transportation infrastructure's capacity, and with ports, state governments, and the federal government all searching for additional investment capital to meet the nation's maritime transportation infrastructure needs and to keep American commerce competitive in the global market.

This nation is not at risk from foreign capital being invested in it, but it would be at risk if it were to discourage continued foreign investment in the maritime industry serving its needs.

There is another aspect to the recent Congressional interest in foreign ownership of marine terminal operators that has been myopic. In addition to the Dubai Ports World-P&O Ports transaction being mischaracterized as a purchase of U.S. ports – which it was not, and in addition to the fact that no facts were provided that showed DPW to be a security risk as a terminal operator – and in fact Dubai was shown to be an important ally and supporter of U.S. efforts in the Middle East and one which is trusted by the U.S. military to service its vessels and cargo, the entire controversy ignored the fact that, even with the six U.S. marine terminals being spun off from this purchase, DPW will be the third largest marine terminal operator in the world, and will be loading cargo onto vessels destined for the United States from its facilities in Australia, Europe, Asia and the Caribbean every day.

Wouldn't it make sense for the U.S. security strategy to try to include companies like DPW as partners of the government's efforts to secure international commerce? DPW is a knowledgeable and professional actor, both globally and in a particularly relevant part of the world. Instead, the Congress just told the third largest terminal operator in the world that it did not trust them, when the facts presented did not justify such a judgment of the company. The unfortunate treatment of this transaction should be kept confined to the narrowest possible application.

---

liner shipping industry transports roughly 11 million containers of imported goods per year to American importers and consumers, 7 million containers of exported goods from American businesses, and important government and military cargoes. The value of this goods movement is over $1.5 billion per day, and these supply chains connect the American economy to the rest of the world. The industry that is responsible for this transportation service is critical infrastructure.

[6] The hundreds of millions of dollars presently being invested in Portsmouth, Virginia by Maersk, in Mobile, Alabama by Maersk and CMA-CGM, and in Jacksonville, Florida by MOL are just three examples of this ongoing commitment to the construction of improved U.S. transportation infrastructure.

The international shipping industry and America's foreign commerce are global enterprises. Devising and implementing effective maritime security enhancements requires the participation and effort of many governments and many foreign owned and operated business enterprises. The U.S. government does not have the capability or the jurisdiction to do this by itself. It needs the cooperation and assistance of foreign governments and foreign owned businesses. The Coast Guard and Customs and Border Protection fully recognize this and are working to build and enhance global security strategies. Protectionism and unfounded criticism of foreign owned enterprises will impair those efforts and will impair security enhancement efforts.

Committee Question #3: The possible impact of terrorists smuggling a Weapon of Mass Destruction via a maritime container on global trade

The shipping industry does not know if terrorists have weapons of mass destruction, or, if they did, the likelihood that a maritime container would be used as a conduit for the transportation or delivery of such a weapon. Terrorists generally do not surrender operational control of their means of delivering an attack, and they would have to successfully evade multiple layers of security measures to succeed.

As I noted earlier, 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 containers. At the same time, America's supply chains extend to tens of thousands of different points around the world, and the potential vulnerability of containerized transportation 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. The impact of such a possible event would be so obviously substantial, however, that there is no choice but to try to design, implement, and constantly enhance a security regime that is effective and still facilitates the efficient flow of commerce.

Committee Questions # 4 and 5: The use of radiation detection equipment and its impact on the flow of commerce, and the Hong Kong container screening concept (Integrated Container Inspection System (ICIS))

Container inspection technologies, including non-intrusive inspection (NII) equipment and radiation screening equipment, clearly have an important role in increasing both the efficiency of inspecting containerized cargo shipments and the number of containers that can be inspected. Container inspection technology, particularly NII equipment, is of substantial interest because, unlike so many other technologies, it helps address the container security question of paramount importance, namely: "What's in the box?"

Container inspection equipment is being deployed at U.S. and foreign ports.

At U.S ports, CBP has reportedly deployed 170 large scale non-intrusive inspection devices. NII inspection equipment allows Customs authorities to have a visual image of a container's contents, is a relatively easy way to review a container's contents in contrast to physically devanning the cargo, and is usually adequate for inspecting a container considered to be of security interest.

The CBP strategy is to inspect 100% of the containers that raise security questions, plus some random inspections. We understand that this comprises about 5.5% of all containers, which would be roughly 600,000 containers a year. These containers are generally subject to delays of 1-3 days in the U.S. port in order to perform the inspection, and the average cost of these inspections appears to range between $100 and $125 per container.

CBP is also deploying radiation scanning equipment at all major U.S container ports. CBP has reportedly deployed 190 radiation portal monitors at seaports to date, allowing it to scan 44 percent of arriving international cargo containers. CBP reports that this percentage will continue to grow through the remainder of this year and 2007, allowing CBP by December 2007 reportedly to scan almost all inbound cargo. The Subcommittee may wish to satisfy itself that this CBP radiation scanning plan is on schedule. CBP also has the ability to use portable devices to detect the presence of radiation, and CBP has issued over 12,000 hand-held devices to its officers with more on the way.

Radiation scanning of containers when performed at the marine terminal gate does not generally delay commerce. Deploying the technology inside terminals to also cover containers moving by on-dock rail shipment has proved more challenging.

CBP and the Department of Energy are also working with foreign ports to install NII and radiation scanning technology abroad as well. Availability of such technology is one of the criteria that a foreign port must meet to become a CSI port, for example.

The "ICIS concept" envisions the installation and operation of radiation and NII inspection equipment by marine terminal operators at foreign ports of loading, the capturing of the NII and radiation scanning images of all containers before vessel loading, the sharing and transmittal of those images to Customs authorities, and the analysis and operational use of those images in the before-vessel-loading security screening process.

This is a concept that has many potential attractions and benefits. It holds the promise of providing the ability to conduct pre-vessel loading inspections of containers entering a port facility without significant delay to commerce, and facilitating the implementation of a more effective supply chain security strategy. Such capability could enable the government to "flex" its security screening capabilities, to inspect more containers, even from a remote location, and to inspect more containers before vessel loading, rather than waiting until they arrive in the United States discharge port.

That latter point is an important one. The current U.S. container security strategy, which the Council completely supports, is to perform container security screening *before* vessel loading in the foreign port. Today, however, most container inspection and radiation screening is performed in the U.S. port of discharge. The ICIS concept would allow for much better alignment between the strategy of screening cargo containers for security risks before vessel loading and the actual capability to perform any desired inspections of such containers before vessel loading.

CBP and DHS officials are presently reviewing this technology and the pilot application of radiation-NII inspection technology to containers entering two Hong Kong port facilities. The technology is conceptually very attractive, but a real world evaluation of the technology, its effect on operations, and its integration into and use by the government is clearly needed. The following issues will have to be addressed in assessing this concept:

1. *Does the technology provide satisfactory quality and technical results?*

This is an issue requiring expert analysis that is beyond the Council's competence. We understand, however, that the preliminary review indicates that both the NII and radiation scanning products are satisfactory from a technical and quality perspective. At the same time, we note that container inspection technology will have to meet defined standards and will not remain static but be constantly refined and improved with time. We also note that there must be multiple, competitive suppliers of the inspection equipment.

2. *Is the U.S. government willing to partner and work with foreign owned and operated marine terminal operators, or will it reject them as untrustworthy?*

The "ICIS concept", as presently articulated, envisions foreign terminal operators installing and operating this inspection equipment. The recent DPW affair has clearly raised the question of whether Congress is willing to accept such a role for these companies. Will Congress accept DPW and other foreign owned terminal operators in such a role? If not, the concept as presently defined would not appear viable.[7]

3. *What is the incentive/reason that will cause marine terminal operators to install and operate such equipment?*

Assuming the U.S. government would tell terminal operators around the world that they would like them to undertake this role, its implementation would require

[7] As we understand the "ICIS concept", foreign governments' approval would be needed for the installation of the system and the operating protocols to support it, but it is not envisioned that foreign governments would be the parties purchasing and operating the equipment. An international agreement amongst trading nations for Customs authorities to purchase, install and operate such equipment on a close to universal scale is conceivable, but is not what we understand the present concept to involve.

these terminal operators to incur significant costs. We do not presently understand the "ICIS concept" to involve the U.S. government funding the purchase, installation and operation of the equipment. A commercial, profit motive of terminal operators' charging $X per container may be sufficient for them to participate in this concept, but the terminal operators are also likely to want to know: whether there are other incentives or reasons to install and operate the equipment; whether the concept if implemented has negative competitive consequences vis-à-vis terminal operators that do not install and operate such equipment; system costs, including how often the government might change the standards of the equipment it would like to see used; and, what kind of operational implications the installation and use of the equipment and system would have on their terminals, including how anomalies resulting from the equipment readings will be resolved.

4. *How is the data transmitted to Customs and Border Protection, and what are the protocols governing what CBP would be expected to do with it?*

The data files generated for millions of containers per year would not be insignificant, and practical technical data issues about the transmittal, storage, and retrieval of this data need to be understood. Are all images transmitted to CBP? Are all the images or readings that meet some particular criteria, such as a particular radiation reading, be transmitted to CBP? Does the terminal operator hold the images and provide only those requested by CBP? How many other governments will ask the terminal operator for the files?

Scanning luggage for airport security involves a review of an object containing several cubic feet of space. A standard 40 foot container contains over 2,700 cubic feet. We understand a trained CBP expert takes four to six minutes to review these images, and this must be done in conjunction with a review of the bill of lading and other shipping documents. Is image analysis software of reliable quality presently available to CBP to help with the task?

We understand the "ICIS concept" to be one to facilitate CBP inspection of all containers CBP has a question about before vessel loading, not that CBP would be expected to review all the images. Does Congress agree with this understanding?

Finally, CBP must be able to properly perform its risk assessment review of all such images of containers of interest, must be able to inform the carrier of any reason why the container should not be loaded consistent with the present 24 Hour Rule Strategy of completing cargo risk assessment *before* vessel loading, and must have agreed protocols in place with local authorities for the resolution of any security questions that arise. Suggestions that implementation issues in the foreign port of loading don't have to be addressed or that the analytical process and screening decision-making can be performed after the vessel is loaded with the cargo and is sailing for the U.S. are unacceptable from a security, a commercial, and an operating perspective.

5. *What are the protocols for what is to be done when the equipment identifies an anomaly that warrants security review?*

The current Hong Kong pilot project appears to be establishing that technology exists to capture NII images and radiation scans of containers entering a marine terminal via a road, of adequate quality, without unduly slowing down commerce. This is important. But to be useful, the technology must be integrated into an operating system that involves data transmittal, government reviews and approvals, and agreed operational protocols for what is done when the technology detects an anomaly. That remains to be done. Marine terminal operators are not interested or trained to perform the security screening of the NII images or radiation readings themselves, nor would they be likely to want to accept the potential liability for such a responsibility.

Numerous nuisance alarms are certain to occur on a regular basis, and there will need to be clear protocols for how such situations will be addressed and resolved in the foreign ports, and by whom. Tile, marble, porcelain products, kitty litter, broccoli, bananas, and other products can all set off the radiation sensor alarms, even though the cargo may be benign. Understanding how these situations would be resolved and by whom is essential. Clearly the involvement and approval of the foreign governments where the port facilities are located will be needed.

Other issues need to be understood and addressed, including how such technology might be applied to transshipped cargo, and at ports like Singapore and Rotterdam where a high percentage of the cargo does not enter the marine terminal by road through a terminal gate, but rather by barge or vessel.

6. *Does the "ICIS concept" include application to U.S. ports and U.S. export cargo? Would the U.S. agree to foreign governments' requests for reciprocity at U.S. ports?*

The Council strongly both supports the efforts of DHS and CBP to establish a priority analysis and review of this "ICIS concept" and its application and this Subcommittee's interest in the issue. The above questions are not intended to detract from the idea, but only to illustrate that the concept's application and implementation involve a number of significant issues. We are hopeful that they can be addressed satisfactorily, but the concept's implementation will take some time.

Question #6: Potential areas for improvement and recommendations for CSI, C-TPAT and global supply chain security

The maritime security challenge is to build on the fundamentally sound strategic framework that DHS has developed and to continue to make improvements on what has been started. Specifically, we believe that priority DHS consideration should be given to:

1. Improving the cargo shipment data collected and analyzed by CBP's National Targeting Center before vessel loading. If cargo risk assessment is to be a cornerstone of DHS policy -- which we believe is a correct approach, and cargo security screening is to be performed before the cargo is loaded onto a ship destined for the U.S. -- which we also believe is a correct approach, it should be using more complete cargo shipment data to perform the risk assessment than only the ocean carriers' bills of lading;

2. Continue expanding international cooperation through the Container Security Initiative network;

3. Continuing to improve and strengthen the C-TPAT program. CBP's expanded program validation efforts are an important part of this effort;

4. Promulgating regulations to implement the MTSA mandate of maritime Transportation Worker Identification Cards for U.S. port workers; and

5. Undertaking a priority examination of the merits and feasibility of widespread application of ICIS-type container inspection and radiation screening equipment and the interface and use of such equipment by Customs authorities.

Summary

When addressing the issue of international maritime security, we find ourselves dealing with the consequences of two of the more profound dynamics affecting the world today. One is the internationalization 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, a demand that produced more than 11 million U.S. import containers in 2005, and will produce roughly 12 million this year, 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.

Foreign equity in the international maritime transportation business is not the security challenge. It has been and continues to be a major, long-standing and positive contributor to an infrastructure that is essential to the American economy and to U.S. national security, and its interest in ensuring the safety and security of maritime commerce is very strong. After all, without a reliable, secure and efficient maritime transportation system, these companies' businesses are in jeopardy.

Mr. Chairman, the World Shipping Council and its member companies believe that there is no task more important than helping the government develop effective maritime and cargo security initiatives that do not unduly impair the flow of commerce. We are pleased to offer the Committee our views and assistance in this effort.