



WORLD SHIPPING COUNCIL
PARTNERS IN TRADE

Statement of

Christopher Koch

President & CEO
World Shipping Council

Before the

Senate Committee on Commerce, Science and
Transportation

On

Maritime Security and Implementation of the SAFE Port Act

October 2007

I. Introduction

The World Shipping Council is pleased to have the opportunity to submit the following comments to the Committee as it undertakes oversight of the various maritime security programs and issues.

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

Liner shipping is the sector of the maritime shipping industry that offers service based on fixed schedules and itineraries. The World Shipping Council's liner shipping member companies provide an extensive, network of services that connect American

businesses and households to the rest of the world. WSC member lines carry roughly 95% of America's containerized international cargo.¹

Approximately 1,000 ocean-going liner vessels, mostly containerships, make more than 22,000 U.S. port calls each year. More than 50,000 container loads of imports and exports are handled at U.S. ports each day, providing American importers and exporters with efficient transportation services to and from roughly 175 countries. Today, U.S. commerce is served by more than 125 weekly container services, an increase of over 60% since 1999.

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

Liner shipping is the heart of a global transportation system that connects American companies and consumers with the world. More than 70 percent of the \$700 billion in U.S. ocean-borne commerce is transported via liner shipping companies.

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

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

II. The Focus on Maritime Security

For the past six years, the WSC and its member companies have strongly supported the various efforts of the U.S. Coast Guard and U.S. Customs and Border Protection (CBP) to enhance maritime and cargo security. The multi-faceted and risk-based strategies and programs of the government have been able to make substantial progress toward meeting this challenge and continue to evolve. At the same time, the Coast Guard and CBP recognize the fact that the industry is transporting on average roughly 50,000 containers, holding roughly \$1.3 billion worth of cargo owned by U.S. importers and exporters, each day through U.S. ports. Significant delays to this flow of legitimate commerce could have substantial adverse effects on the American economy.

The multi-layered maritime security strategy has a number of parts on which I will briefly comment today. The basic architecture of U.S. maritime security is well known and understandable. First, there is *vessel and port security*, overseen by the Coast Guard and guided in large measure by the International Ship and Port Facility Security Code (ISPS). Second, there is *personnel security*, overseen by various Department of Homeland Security agencies and the State Department. Third, is *cargo security*, which

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

with regard to containerized cargo, is addressed through Customs and Border Protection's advance cargo screening initiative, C-TPAT, and the Container Security Initiative – all of which are reinforced and made more effective by the increased deployment of container inspection technology at U.S. and foreign ports.

A. Vessel and Port Security Plans

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

The liner shipping industry's operations are consistent and repetitive – its vessel services and crews call at the same ports every week. So long as there is consistent and professional implementation of the security rules, which is a hallmark of the Coast Guard, liner shipping has found no problem in operating in the new vessel or port security environment.

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

Long Range Information and Tracking (LRIT) of Vessels: On October 3, the Coast Guard published a Notice of Proposed Rulemaking (NPRM) on Long Range Information and Tracking (LRIT) in the Federal Register. The Council supports the LRIT objective and the enhanced visibility of vessels offshore that it will give to the Coast Guard and other governments.

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

There may be concern, however, regarding how the Coast Guard intends to implement LRIT if the international operating system envisioned by the International Maritime Organization's (IMO) LRIT Convention is not in place. The International Mobile Satellite Organization (IMSO) has been designated as the entity to run LRIT for the IMO. A request for proposals has been issued to build the LRIT system, but it is our understanding that the technology vendor(s) have not yet been selected, and that construction of the LRIT system has not yet commenced. A uniform, global operating system is the desired objective. Different nations establishing unilateral systems could present legal and operating challenges. The Coast Guard has invited comments on these issues in its recent NPRM, and we expect that the industry and other governments will be considering these issues closely.

Small Vessels: The attacks on the *U.S.S. Cole* and *M/V Lindbergh* demonstrated that large vessels can be the objects of terrorist attack from small boats. The U.S. Coast

Guard Commandant, Admiral Allen, has on numerous occasions noted this and other small boat vulnerabilities and the difficulty in devising effective ways to address the threat without significantly inconveniencing recreational and small boat movements. The Council notes that DHS has recently undertaken some pilot efforts on the West Coast to test technologies that may contribute to addressing this issue, and while we recognize the difficulty of the challenge, we believe that such DHS effort are focusing on a legitimate concern. We also appreciate that the U.S. Coast Guard is playing a lead role in having put this on the International Maritime Organization's agenda in order to develop international principles and criteria for addressing this issue.

B. Transport Worker Identification Credential

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

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

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

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

Lastly, DHS has also announced it will begin to enroll workers in Wilmington, Delaware starting on October 16, and has also listed the next eleven follow-on locations for enrollment. The industry strongly supports a measured implementation of this challenging new regime so that any unanticipated issues that may arise can be addressed as the system is rolled out in stages.

C. Containerized Cargo Security

The WSC fully supports the U.S. government's strategy in addressing containerized cargo security. Specifically, the Council supports CBP's risk assessment and screening of 100% of all containers prior to their being loaded onto vessels destined for the U.S., and the pre-vessel loading inspection of 100% of those containers that CBP's cargo risk assessment system determines to present a significant security risk or question. The Council does not support recent legislation's call for inspection of 100% of all import containers before vessel loading, because the concept has not been clearly considered and remains presently impractical.

1. Container Security Initiative (CSI)

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

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

2. Containerized Cargo Screening and Risk Assessment

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

C-TPAT: One element of that system is the Customs' Trade Partnership Against Terrorism (C-TPAT) pursuant to which various entities in the supply chain voluntarily undertake security enhancing measures. CBP then validates participants' compliance, and compliant supply chains are accordingly afforded lower risk assessments.

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

Better Security Screening Data: "10 plus 2" Initiative: While the 24 Hour Rule has been in the Council's view a logical and sound effort, the Council has for several

years noted that more effective advance cargo security screening will require more data than the information provided by carriers via the 24 Hour Rule

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

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

Customs and Border Protection (CBP) is developing a regulatory proposal that would require U.S. importers or cargo owners to file ten additional data elements² with CBP 24 hours prior to vessel loading, and to require ocean carriers to provide two additional sources of data -- vessel stowage plans prior to arrival in the U.S., as well copies of electronic container status messages. This is referred to as the "10 plus 2" initiative.

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

While the private sector obviously needs to await the actual proposed regulation before providing comments in the expected rulemaking, we would note that CBP's efforts in developing this initiative have been transparent, professional and cooperative, and are in pursuit of a strategic objective that is not only mandated by the SAFE Port Act, but is highly logical in order to enhance containerized cargo risk screening.

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

This initiative has not yet been clearly explained to the industry, and there has not yet been any public transparency or opportunity to comment on the initiative.

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

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

What services, analysis or risk assessment competence would be required of such vendors is unclear. What the specific data to be gathered would be has not been explained. The extent to which such shipment data would be shared with other governments is not clear. How this system would be integrated into CBP's existing Automated Targeting System is unclear. How such a commercial third party data manager would make money off this program is unclear, and who would bear what costs for participating in such a system is unclear. How the data in the system would be protected is unclear. Whether ocean carriers would be expected or invited to participate in the provision of information is unclear. What benefit would result from participating in such an effort is unclear.

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

In short, the GTX effort has not yet been explained by the government and is not yet understood by the trade. U.S. importers with whom the Council has discussed this initiative are confused by this process. There is concern within the trade community over the apparent development of such an initiative without the government's usual transparency and process of consultation. That concern would likely be exacerbated if public review and comment were not requested, allowed or considered prior to the restricted procurement solicitation that is expected.

3. Container Inspection

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

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

In order to further consider the issues involved in the application of additional container inspection at overseas ports of loading, DHS has undertaken the "Secure Freight Initiative", under which pilot projects are being established at several foreign ports testing more complete pre-vessel loading scanning, generating possible lessons to

be learned for broader application of pre-vessel loading container inspection efforts.³

The “Implementing the 9/11 Commission Recommendations Act”, which was signed into law in August, includes the well known provision requiring that by 2012 100% of the containers imported into the United States be “scanned” before being loaded aboard vessels destined for the United States, meaning that the container would have to be run through radiation detection equipment *and* non-intrusive imaging equipment before vessel loading. What, if anything, would be done with the images or data produced by those scanings was not addressed by the law, nor were a host of other highly relevant questions, including who was to perform this task, and whether the U.S. would perform such scanning of its own export containerized cargo. The WSC issued a six page statement on this legislation on July 30th, which is attached to this testimony as Attachment A.

A number of other governments are obviously and justifiably concerned about the implications and meaning of this new U.S. law. We expect that they will continue to inform the U.S. government of their concerns, including their view that this statutory provision expects foreign governments to undertake measures for their exports that the U.S. government has no intention to undertake for its exports. The shipping industry’s customers -- the hundreds of thousands of U.S. importers and exporters who use containers to transport their cargo, are also concerned about the potential effects of this law.

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

4. Seals and Container Security Devices

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

Accordingly, the “9/11 Commission Recommendations Act”, Congress amended this section by providing that: “(B) Interim Requirement.-- If the interim final rule

³ DHS has established three full scale container scanning pilots in co-operation with host governments at Southampton, U.K.; Puerto Cortes, Honduras and Port Qasim, Pakistan. Honduras and Pakistan are operational, with the UK scheduled to come online shortly. Three other smaller scale pilots are under development at port facilities in Busan, South Korea (Gamman Terminal); Salalah, Oman, and Singapore.

described ... is not issued by April 1, 2008, then effective not later than October 15, 2008, all containers in transit to the United States shall be required to meet the requirements of International Organization for Standardization Publicly Available Specification 17712 standard for sealing containers....” Thus by next October all U.S. inbound containers will be required at a minimum to have ISO standard security seals.

As to the government’s view of “*container security devices*” (CSDs), things are less clear. The Council has understood that DHS was planning to issue proposed draft technical requirements for container security devices and the operating protocols associated with such devices by the end of this year for public review and comment. We understand that the DHS Science and Technology directorate prepared a draft of such requirements that is undergoing further review and amendment within the Department.

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

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

There has been little light or transparency provided on these issues, although in fairness, they are not simple issues. The Council believes it is essential, if an interest in CSDs is to be pursued, for the government to undertake a fully transparent and very clear articulation of its draft views on the requirements for such technology and the related operating systems and protocols, and to provide the public with a meaningful opportunity to comment upon such draft requirements, *before* they are advanced as an element of the government’s container security strategy.

D. Port of New York’s Recommendation for New Container Taxes

At the Committee’s hearing on October 4, the witness for the Port Authority of New York and New Jersey expressed support for new “legislation establishing a uniform, nationwide Port Security User Fee to help offset growing port security costs.”

This is a bad idea for many reasons.

First, it is relevant to note that the view of the Port of New York’s witness at the hearing is not the position of the American Association of Port Authorities.

Second, when the Coast Guard promulgated its maritime security regulations in 2003 implementing the Maritime Transportation Security Act of 2002, it projected that the

cost of compliance for the industry would be \$7.331 billion over 10 years.⁴ The New York Port Authority witness stated that the federal government has provided \$1.3 billion in port security grants over the past five years, which is only a “fraction of the security costs that the industry has incurred over the same period” and that the regulations are an “unfunded mandate that industry has to bear”.

The Coast Guard’s cost estimates were of what the *industry* was going to have to spend to comply with its regulations, not the amount of money the government needed to provide the nation’s ports. Further, most of these expenses are already being incurred by the private sector carriers, terminal operators and cargo owners, without any federal assistance.

Under the rationale of the Port of New York, it would appear that every regulation the government produces that has compliance costs is an “unfunded mandate”. It seems a novel proposition indeed that the federal government should be responsible for all the costs that industry incurs in complying with government regulatory requirements. It is frankly illogical to argue that because the industry’s regulatory compliance costs are X, and the government has provided grants in an amount which less than X, that we need a new federal tax to make up the difference. We believe that the port industry should be appreciative for the grants that have been provided, particularly considering that there has never been a very precise delineation of what port security grants should be used for.

Shippers, forwarders, brokers, carriers and marine terminal operators have all incurred substantial costs to comply with applicable security regulations and programs. They have not asked the government to pay for those compliance costs, What they do want is for the requirements to be well designed to improve security in a cost-effective manner.

Third, the Port of New York witness did not identify with any specificity what such federal port security grant money is needed for, or why it is the responsibility of all cargo containers across the nation to provide it. We appreciate that the Port of New York witness notes that entities in the Port of New York and New Jersey have received 12% of total port security grant funding and that the Port apparently believes that it should receive a higher share; however, as explained below, there is an existing mechanism for the port to increase its revenue collection to cover higher costs if it is important to do so.

Fourth, and perhaps most importantly, ports currently have and use the authority and capability to collect additional funds they need for security at their facilities from their commercial customers. Today, as the Port of New York witness noted, ports throughout the U.S. and abroad are assessing and collecting port security charges from their commercial customers. They also have antitrust immunity under the Shipping Act to collectively establish such charges if they wish to do so. There is no need for a new federal tax. Though questions of equity and appropriateness of such fees obviously should be addressed on a case-by-case basis, the very fact that the ports’ customers, including the members of the World Shipping Council, are presently paying these port

⁴ First year estimated cost of implementation was approximately \$1.5 billion, with an annual cost of approximately \$884 million. Implementation of National Maritime Security Initiatives, 68 Fed.Reg. 60448, 60464 (Oct. 22, 2003).

security fees belies the notion that extensive new federal taxes or “user fees” warranted.

Finally, the Port of New York witness noted concern that U.S. seaports should not be put at a “serious disadvantage in relation to ports in Canada and Mexico.” We question whether ports such as Seattle and Tacoma would see a new national tax on commerce going through their ports to pay for more grants to the Port of New York as doing anything other than disadvantaging them in relation to ports in Canada.

III. Conclusion

Vigilance against terrorist risks requires the development and implementation of prudent security measures, and the continuing enhancement of such measures as the risks change and take new forms. The international trading system is too valuable and important to be left unattended.

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

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

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

1. There is a clear and specific definition and agreement on what should be done to improve security.
2. There is a clear and thoughtful prioritization of initiatives.
3. There is sufficient certainty and clarity in purpose to do it right. In the absence of that, time and resources are poorly used and the efforts are less likely to improve security.

We appreciate the Subcommittee’s continued interest and oversight of these issues, and would be pleased to provide additional information that may be of assistance to the government in addressing these issues.

Attachment A



Statement Regarding Legislation to Require 100% Container Scanning

July 30, 2007

The first session of the 110th Congress has enacted H.R. 1, the “9/11 Commission Recommendations” legislation, which the President has said he will sign. Included in that legislation is a provision, which was *not* a recommendation of the 9/11 Commission, that requires, effective July 2012, that all maritime cargo containers being imported into the United States must be “scanned” at foreign ports of loading or they will be denied entry into the country.

This so-called “100% scanning”, or “100% container inspection” requirement as it is sometimes called, was opposed by the Department of Homeland Security (DHS), Customs and Border Protection, present and former government security experts, the U.S. Chamber of Commerce, all major cargo shipper organizations, the ocean carriers transporting the cargo, as well as the European Commission and the governments of America’s trading partners, including Belgium, Canada, Denmark, Finland, France, Germany, Greece, Italy, Japan, the Netherlands, Norway, Poland, Portugal, Singapore, Spain, Sweden, and the United Kingdom.

Why was such a proposal opposed by virtually all elements of the global trading system? Was it because of cost? No. Was it because of a lack of commitment to enhancing cargo security? No. It was in the words of the *Washington Post* “a bad idea” and “a slogan not a solution”. It was because the legislation is not only unworkable, but that the Congress failed to even try to address fundamentally critical questions about how such a system would actually operate.

The New Law

The legislation provides:

“(1) In General.—A container that was loaded on a vessel in a foreign port shall not enter the United States (either directly or via a

foreign port) unless the container was scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel. (2) Application.—Paragraph (1) shall apply with respect to containers loaded on a vessel in a foreign country on or after the earlier of —(A) July 1, 2012; or (B) such other date as may be established by the Secretary under paragraph (3).”

The Problems

The House passed H.R. 1 without having Committee hearings or allowing floor amendments on this issue. The Senate did not have a hearing on these issues.

Nevertheless, every one of the following issues was repeatedly brought to the attention of the Congress by numerous parties, but without effect.

1) Pilot Programs Ignored: Pursuant to the SAFE Port Act passed by the Congress just last year, the Department of Homeland Security has established pilot programs under the “Secure Freight Initiative” in a number of ports around the world to test the concept of scanning containers loaded onto ships destined for the U.S. Those pilots are still underway, and their lessons have not been examined or considered.

2) Failure to Define Who is To Perform the Container Scanning: It would seem elementary that U.S. legislation requiring every container to be scanned before being loaded onto a vessel in a foreign port would address the issue of who is to perform this activity. This legislation fails to do so. It does not require U.S. Customs to do this, as it is clearly impossible for the Congress to require U.S. Customs to undertake such activities within the jurisdiction of other sovereign nations. It does not require foreign governments to do so, as it has no such authority. The legislation simply says that containers shall be scanned. By whom? By governments? By foreign port facility operators? The Members of Congress sponsoring this legislation took the position only last Congress that one of the largest port facility operators in the world, Dubai Ports World, was an unacceptable security risk to buy a U.S. marine terminal operating company and hire U.S. workers to service vessels in U.S. ports. Is that company, and other private terminal operating companies, now who Congress looks to scan U.S. bound containers in foreign ports? Does Congress care who performs this activity? If Dubai Ports World now undertook this role, would the Congress approve such a role? One would think such a basic question would have been subject to some examination by the Congress and some answers.

3) Failure to Define Who is to Purchase, Operate and Maintain the Technology: Related to the above question, is the failure of the legislation to define who is expected to undertake the substantial capital commitments and operational responsibilities to implement such a system.

4) Failure to Address Health and Safety Issues: The legislation fails to recognize the need to address the health and safety issues relating to the use of this equipment. Even if the equipment performs to the U.S. government’s health and safety regulatory requirements, other governments have different standards. Furthermore, labor and workforce acceptance of driving through non-intrusive imaging (NII) equipment remains a significant issue. U.S. port labor will not do so. As a practical matter, this

legislation requires the rest of the world to do what cannot be done today in U.S. ports.

5) Failure to Seek or Obtain the Necessary Cooperation of Other Governments: No expansion of overseas container inspection will occur without the cooperation and consent of foreign governments. This law fails to even acknowledge the need for their cooperation. Customs and Border Protection has spent considerable effort since 9/11 to build cooperative bilateral Customs-to-Customs working agreements at seaports around the world through its Container Security Initiative (CSI). The success of CSI is based on mutual respect, recognition of other nations' sovereignty, cost sharing, and targeted priorities. This legislative mandate is devoid of those qualities.

6) Failure to "Practice What You Preach" – No Reciprocity: Congress was repeatedly advised of the difficulty of this legislation's requiring 600 ports around the world to approve, implement and utilize such technology, systems and processes for all cargo destined for the U.S. or effectively face an embargo on their exports, when the U.S. government does not even try to perform this function on its export cargo, scans virtually zero U.S. export containers, and has no plans to do so. If implementation of this law is actually pursued, it is entirely possible, if not highly likely, that foreign governments would establish "mirror image" requirements on the U.S., forcing all American export containers to undergo radiation and NII scanning before vessel loading at U.S. ports -- requirements which the U.S. government and U.S. port facility operators are presently and for the foreseeable future incapable of meeting.

7) Failure to Define the Scanning Requirement: Congress recognized that 100% container "inspection" is impractical and therefore requires instead that every container be "scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel." This by itself would be pointless. The law fails to address what is to be done with the scanning data generated, whether or when the data from the scanning equipment is transmitted to the U.S. government, or who is to analyze the data generated.

8) Failure to Address Scanning Analysis Responsibility: The law fails to address whether the scanning data actually has to be reviewed and analyzed, and if so, under what circumstance, when and by whom? In essence, it fails to identify how the technology is to be used. Will the images of every scanned container have to be reviewed? If not, when are the images to be reviewed and by whom? Are they simply to be filed in an electronic library somewhere? If so, is it reasonable to ask other nations to invest hundreds of millions of dollars in such equipment, plus labor, maintenance and operating costs, if these images will only be used on an exception basis or for "forensics"? This cost/benefit question is even more relevant in light of Members of Congress' criticisms of the efficacy of the equipment currently being used for these purposes by DHS, especially after questions about such equipment were recently raised by the Government Accountability Office. Further, the law fails to try to address what is done if one of the scans identifies an anomaly that requires secondary inspection – a common occurrence with the use of these technologies. These are fundamentally important issues with difficult operating protocols and significant costs associated with them – all of which the legislation does not address.

“Extension” Authority

Recognizing that this legislation has fundamental problems, some have noted that the law grants the Department of Homeland Security discretion to extend the effective date of the requirement. Before examining that part of the legislation, it is important to note that the law does not allow DHS to amend or adjust the law’s requirement, only to extend the effective date of the 100% container scanning requirement.

The law provides:

“Extensions.—The Secretary may extend the date specified in paragraph (2)(A) or (2)(B) for 2 years, and may renew the extension in additional 2-year increments, for containers loaded in a port or ports, if the Secretary certifies to Congress that at least two of the following conditions exist:

“(A) Systems to scan containers in accordance with paragraph (1) are not available for purchase and installation.

“(B) Systems to scan containers in accordance with paragraph (1) do not have a sufficiently low false alarm rate for use in the supply chain.

“(C) Systems to scan containers in accordance with paragraph (1) cannot be purchased, deployed or operated at ports overseas, including, if applicable, because a port does not have the physical characteristics to install such a system.

“(D) Systems to scan containers in accordance with paragraph (1) cannot be integrated, as necessary, with existing systems.

“(E) Use of systems that are available to scan containers in accordance with paragraph (1) will significantly impact trade capacity and the flow of cargo.

“(F) Systems to scan containers in accordance with paragraph (1) do not adequately provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.”

It is presumably the ambiguity and flexibility of this language that has allowed the President to sign this legislation, as it might be used to extend these requirements, perhaps indefinitely, although that is not clear and could be arguable.

Criteria (A) would seem meaningless as a justification for extension, as radiation and NII scanning systems are “available”. Criteria (C) is of limited application because ports’ “physical characteristics” are not generally among the principal issues involved with implementing such a concept. Criteria (D) does not define what “existing systems” means. Criteria (B) and (F) are confusing because NII scanning equipment, unlike radiation scanning equipment, neither produces “alarms” nor “automatic notification of

questionable or higher risk cargo". So what does this mean?

Without belaboring the point, the "extension" authority portion of the legislation is unclear, but the Administration would seem to have some ability to avoid application of the implementation date of the law.

It is therefore odd, disconcerting, yet entirely predictable that this legislation produces both statements from Members of Congress that the law will require 100% container scanning at foreign ports by 2012, and statements from other observers that the law is wholly impractical and thus it is unlikely to be applied because the U.S. government will not cut off its own commerce with countries that do not implement 100% container scanning before vessel loading.

This provides little comfort or certainty to governments and ports around the world that are trying to understand what this legislation passed by the Congress of the United States actually means and what its implications are.

The Path Forward

Roughly \$500 billion of annual American commerce is affected by this law.

What is clear is that this issue deserved a more open process of analysis and debate, that other governments resent the unilateral dictates and hypocrisy in the law, and that there are over 600 ports around the world trying to figure out what this legislation means.

The issue of how to continuously improve containerized cargo security is important to the American public, to American commerce, and to the shippers and carriers and ports involved.

There are a range of existing efforts to address this challenge, including:

- the "24 Hour Rule" and the advance screening and risk assessment of cargo shipment information before vessel loading for 100% of all containers coming to the U.S.:
- the Container Security Initiative noted earlier;
- the Customs Trade Partnership Against Terrorism initiative;
- the radiation screening of virtually every container arriving at a U.S. port;
- the inspection of every container that Customs and Border Protection believes presents a significant security question;
- security plans overseen by the Coast Guard for every vessel entering a U.S. port and every port facility;
- the Department of Energy's "Megaports initiative", which provides radiation detection equipment and trains personnel abroad to check for nuclear materials. In exchange, DOE requires that data be shared on detections and seizures that resulted from the use of the equipment. This initiative and the CSI initiative are collaborative efforts by two different U.S. agencies, DOE and DHS, working with host countries to reduce the risk of terrorism.

- the International Port and Security Program (IPSP) initiative, under which the U.S. Coast Guard and host countries work together to evaluate compliance with the International Ship and Port Facility Security (ISPS) Code. This information improves U.S. and foreign security practices, and helps assess if additional security precautions will be required for vessels arriving in the U.S. from other countries.
- as well as two major emerging DHS initiatives – the “10 plus 2” program, under which Customs and Border Protection will require importers to provide 10 additional data elements before vessel loading for enhanced security targeting and 2 additional streams of operating data from ocean carriers to assist in the tracking of container movements, and the Transportation Worker Identification credential that will provide DHS security screening of transportation workers.

Neither the government nor the industry is ignoring the enhancement of maritime security.

To the extent a vision for 100% container scanning of containers on a global basis is to be moved forward, it will require a more open, consultative examination of the real world issues involved than what transpired in the debate and enactment of H.R. 1.

###