



WORLD SHIPPING COUNCIL
PARTNERS IN AMERICA'S TRADE



THE
NATIONAL
INDUSTRIAL
TRANSPORTATION
LEAGUE

In-Transit Container Security Enhancement

September 9, 2003

Since September 11, 2001, governments and industry have given extensive consideration to the issue of protecting international commerce from terrorist threats. One of the maritime security issues that has been given particular attention is the security of containerized cargo shipments.

The World Shipping Council (Council), the International Mass Retail Association (IMRA), the National Industrial Transportation League (League), and their member companies (hereinafter "the industry") have supported the U.S. government's efforts to establish the "24 hour rule" by which carriers file advance shipment information with the U.S. government 24 hours before loading containerized cargo aboard a ship bound for the U.S., so that the government can conduct a risk-based screening of all such shipments. The industry supports the Container Security Initiative (CSI) establishing government-to-government

agreements addressing data sharing, risk assessment, and cargo screening and, where appropriate, inspection. The industry supports the deployment by governments of more non-intrusive container inspection equipment both here and at foreign loading ports so that any shipment of containerized cargo that warrants inspection can be inspected efficiently and quickly. The industry supports the Customs' Trade Partnership Against Terrorism (C-TPAT) program establishing a government-industry partnership designed to enhance the security of the entire shipment supply chain. The industry continues to support the development and implementation of analogous efforts at the international level through the World Customs Organization. The industry has supported the Coast Guard's vessel and port security initiatives internationally and in domestic rulemakings. The industry supported the creation of the Department of Homeland Security.¹ The industry strongly supports the governments of trading nations establishing predictable and transparent, and mutually consistent, security rules governing these issues.

Two of the most important responsibilities regarding container security are the secure loading (or "stuffing") and sealing of a container by the shipper, and the in-transit security of the container once a carrier picks up the loaded, sealed container from the shipper's premises until the container is delivered to its destination.

The first feature – the secure stuffing of the container – is where container security begins. Without it, in-transit security is obviously of limited value. Carriers do not load the cargo into or seal a container. The shipper performs those functions.

Container security is thus a shared responsibility. The shipper is responsible for stuffing and sealing a safe and secure container. Those who have custody of the container during its transit are responsible for its security in transit. Government also has critical responsibilities, and, with the support of carriers and shippers, it has expanded its capabilities to gather and analyze advance data on all container shipments, screen all such shipments, and inspect any container that raises a security question.

This paper, while recognizing the essential security importance of the container stuffing process and the government cargo screening and inspection processes, does not address those issues. This paper only addresses the issues

¹ Ocean carriers and shippers have supported the Bureau of Customs and Border Protection's ("CBP") development of the 24-hour advance cargo filing rules, the Container Security Initiative, and the C-TPAT program. The industry understands that CBP has responsibility for containerized cargo security within DHS, but also understands that the Transportation Security Administration within DHS has been delegated authority under several sections of the Maritime Transportation Security Act that address containerized cargo security issues. Clarity on the respective roles and responsibilities of TSA and CBP in this regard is needed. This paper assumes that the programs, operating systems, regulations and personnel of CBP would be whom the industry would interface with in implementing these recommendations, but the industry would obviously accommodate a defined TSA role as well.

involved in the following proposed set of protocols and requirements for enhancing the in-transit security of containerized cargo shipments.

In doing so, it should be stressed that the security of container stuffing, the government's risk assessment and cargo screening systems, procedures and capabilities, and the enhanced deployment and use of non-intrusive container inspection equipment are critically important. In-transit security, while important, is not a substitute for these.

This paper submits that the issue of "in-transit" security can best be explored both by considering what can be done in the short term to enhance the in-transit security of loaded containers being shipped to the United States², and what might be a security objective for a future "smart" container. By "short term", we mean hopefully within a year. By "future", we mean within several years, not a vision that may be decades away. The Council, IMRA, and the League offer these views in the hope that they will be useful to the efforts to enhance the security of international commerce and the security of all trading nations' economies.

A. Proposed Short Term Vision

Based on the foregoing, the Council, IMRA, and the League propose for consideration the following updated amplification of the Council's position as set forth in its January 2002 White Paper as a definition of short term requirements that the government should establish for all shippers and carriers:

² This proposed regime would not apply to empty containers. Pursuant to the C-TPAT program, to which all the Council's member companies and many members of IMRA and the League belong, ocean carriers have agreed to inspect all empty containers prior to loading them aboard a vessel, but carriers do not support the application of a requirement to seal empty containers. In fact, carrier security representatives have expressed concern that a blanket requirement to seal empties could create security issues because they could not be easily opened and checked.

In addition, the regime proposed in this document could apply to U.S. export containers. The United States' trading partners could understandably expect the U.S. to apply the same security measures to its export cargo that is applied to its import cargo. We also recognize, however, that there may be issues that could cause some to want to address export shipments separately. In that regard, for example, (1) we are unclear of the capabilities of the Automated Export System (AES) to handle the seal reporting data recommended herein, (2) American exporters would probably need some time to comply because they are less consistent in applying seals to containers than shippers of import containers, particularly shippers of low value export commodities such as waste paper, hay, etc., and (3) a broader seal and "in-transit" security regime may logically need to be developed to apply to all cargo shipments, domestic and export, being transported in containers and in highway trailers within the United States, and not just to containers that are being transported with export cargo.

1. Shipper Obligation To Seal: A shipper³ is responsible for sealing, and should be required by law to seal, a container upon stuffing it. The shipper must provide the seal number on all shipping documents.
2. Seal Standards: All seals must meet a minimum standard. We recommend the ISO standard for high security seals (PAS 17712). We recommend that the government establish a specific date by which all containerized shipments must be affixed with such seals by the shipper. If the shipper chooses, it may use a seal that goes above the minimum standard.
3. Recording Seal Changes: When persons having custody of a container, including U.S., state and local government officials, break the seal for legitimate reasons, they must be required to affix a new seal meeting the ISO standard, and provide the carrier or terminal operator in possession of the container with a written confirmation of the event. The carrier must record the new seal number on the shipping documents.

Recognizing that a U.S. regulation cannot be effectively imposed on persons not subject to U.S. jurisdiction, this requirement should nevertheless apply to all persons within the U.S. and otherwise subject to U.S. jurisdiction. We would support this same set of requirements being applied outside U.S. jurisdiction by other governments so that a common international approach to this issue can be established, and recommend that CBP work to incorporate them in the various CSI agreements with other governments.

4. Modal Changes: The party receiving the container (e.g., trucker, railroad) at each modal interchange⁴ must verify and record the seal, its number and its condition upon receipt of the container. If there is a seal discrepancy or anomaly, the receiving party shall inform the shipper, the party tendering the container, and the party to whom it delivers the container of such discrepancy or anomaly, and shall note the anomaly or seal discrepancy on the shipping documents.
5. Ocean Carrier Seal Verification: The ocean carrier or its agent must verify the seal, meaning that the ocean carrier should determine before loading a container onto a vessel bound for the U.S.:

(a) Whether a proper ISO standard seal is affixed to the container,

³ The term “shipper” in this context is meant to refer to the party responsible for the safe and secure loading or “stuffing” of the container. That party may or may not be the party with whom the carrier has the transportation contract

⁴ “Modal interchange” here would cover the modal transfer of the container from ocean carrier to trucker, trucker to rail, rail to truck, etc, but is not intended to cover rail interline changes where, for example, control of a stacktrain is transferred from one railroad to another railroad.

(b) In the affirmative, whether the seal is intact,

(c) What the seal number is, and

(d) Whether that seal number is the same as the shipper has stated in the shipping documents it originally affixed to the container.⁵

This verification may occur at the marine terminal gate or after entry to the terminal but before vessel loading. If the marine terminal at which the vessel loading occurs does not have a terminal security plan that conforms to the ISPS Code or is determined by the U.S. or foreign government to be not adequately secure, then CBP, in consultation and coordination with the U.S. Coast Guard which has regulatory responsibilities for foreign port assessments, should include that factor in its Automated Targeting System (ATS) to determine the appropriate treatment of the container.

For U.S. bound containers that arrive at a foreign marine terminal via on-dock rail rather than through the terminal gate, the carrier or its agent should be required to conduct a seal verification of such containers in the terminal before vessel loading.

For U.S. bound containers that are relayed from a vessel or barge at a foreign marine terminal, the carrier or its agent should be required to have the seals verified in the terminal before vessel loading, unless the carrier has verifiable procedures in place to ensure that the container seal was previously checked at the marine terminal where the container was originally loaded onto the relay vessel or barge.⁶

The carrier should have a compliance program to ensure that the seal verifications are performed.

If the above can be verified through manual procedures, that should be acceptable. If the above can be verified in the future through electronic means, that should be acceptable. The industry must have the flexibility to decide when it is most appropriate to use e-seal technology to accomplish these checks.⁷

⁵ There will be some situations where the carrier may not be able to verify the match of the seal numbers until after the vessel is loaded. For example, the seal number provided by the shipper may be duly recorded in the shipping documents and provided to CBP via the AMS system 24 hours before vessel loading. An hour before vessel loading, the container arrives through the marine terminal gate, the seal number is read and entered into the terminal operator's system. The transfer of the data from the marine terminal operator to the carrier and the cross-referencing of the seal number in the carrier's system may not be completed until after vessel loading has completed. In that situation, the carrier could promptly report the fact and any explanation it receives to CBP via the AMS system, so that, if there is an inadequate explanation of the discrepancy by the time the ship arrives, CBP can inspect the container at the U.S. port of discharge.

⁶ These procedures could be included in the vessel carrier's C-TPAT security plan.

⁷ See additional discussion of electronic seals in Part B.

6. Requirement of Seal to Load Aboard the Vessel: The government should establish a requirement that no loaded container be stowed aboard a vessel without an intact, conforming seal.
7. Addressing Seal Anomalies: If a carrier receives a loaded container with a seal that does not meet the ISO standard referenced above, the carrier shall leave the nonconforming seal in place, and shall apply an ISO standard seal. The carrier shall record the new seal number on the bill of lading, and inform CBP of the fact in its AMS filing. CBP should consider such information in its ATS profiling of container shipments.⁸

If during or after seal verification, the carrier finds a seal discrepancy or a broken or missing seal, the carrier shall attempt to obtain an explanation of the anomaly.⁹ In the event of a seal anomaly, the carrier shall notify CBP of the anomaly and the explanation it has received via AMS. Such notification shall not start a new 24-hour clock. CBP is requested to program the AMS data field for seal information to accommodate written textual explanations in order to accomplish this. CPB may order the inspection of any container that has had a seal anomaly at CSI loading ports or at the U.S. port of discharge.¹⁰

⁸ Item 1 recommends that a shipper be required to seal the container upon stuffing it. Recognizing that there are limits to the government's jurisdiction to regulate conduct in other countries, we nevertheless believe that it is important for CBP to establish significant consequences for cargo interests if they do not fulfill their security obligation and apply a proper seal upon stuffing the container. If the carrier addresses the problem of non-standard seals by putting an ISO standard seal on the container, and there are no consequences to the shipper or the consignee, then inadequate compliance will result.

⁹ It is important to recognize that there are seal changes on hundreds of thousands of container cargo shipments in U.S. commerce each year, and the vast majority of them do not give rise to security concerns. In some countries, local Customs officials will break the seal on every export container and affix a new seal. Seals are security indicators; however, just as an intact seal does not guarantee that a shipment hasn't been tampered with, a changed seal does not necessarily mean that there is a security problem with a container. The industry nevertheless believes that there would be security value in governments establishing uniform, consistent, seal protocol requirements as recommended herein.

¹⁰ The industry considered recommending that any seal discrepancy be provided to CBP pursuant to the 24-hour rule and carriers be allowed to load unless CBP said not to, but that could require all containers to be received in the marine terminal considerably earlier than 24 hours before loading and probably roughly 48 hours before vessel loading. This would present serious operational limitations and delays to commerce. The industry also considered holding all containers with seal anomalies until CBP provided an affirmative OK to load, but believe from experience, from the numbers of seal anomalies that do occur without security implications, and from CBP's responses pursuant to 24 hour rule questions, that this would overwhelm CBP and delay commerce unnecessarily. CBP retains the ability to inspect a container with a seal anomaly at the U.S. port of discharge.

Implementation of Proposed Short Term Vision

We propose a consultative, government-industry planning process for the development of an implementation schedule for these proposed requirements, which should address, inter alia:

- The most appropriate authority under which the government should promulgate the requirements proposed in Items 1-7 above¹¹,
- The schedule for CBP's information systems to be reprogrammed to accept the additional seal data proposed,
- An implementation schedule for port and marine terminal operators who would need to change their processes or technologies to accomplish the above,
- The international review and adoption of such requirements through a predictable, transparent, and mutually consistent approach.

B. Electronic Seals

Electronic seals have not been proven to provide any greater security than mechanical seals.¹² It is highly unlikely that an electronic seal product meeting technical, operational, standard-setting and economic criteria can be developed, agreed upon and implemented within the twelve month goal of the proposed short term vision discussed above. Carriers and shippers, however, may want to consider the option of using e-seals to implement the above. In considering that possibility, and because of the interest in the issue of e-seals, the industry's members have considered that an e-seal should possess the following security characteristics:

- (a) Have a unique seal number that can be BOTH electronically read and can be read visually, as it is wholly impractical to have electronic readers at all relevant points;
- (b) Record the date and time when the seal was activated or sealed;
- (c) Record the date and time when the seal was opened or breached;

¹¹ See footnote 1.

¹² It is important to recognize that e-seals are not necessarily a solution to containerized cargo security concerns. As a report by the Vulnerability Assessment Team at the Los Alamos National Laboratory states: "High-tech electronic seals are not automatically better than simple mechanical seals, and are often worse." *"Tamper-Indicating Seals: Practices, Problems and Standards"*, by Roger G. Johnston, Ph.D., Vulnerability Assessment Team. Los Alamos National Laboratory, Los Alamos, New Mexico. Prepared for the World Customs Organization Task Force on Security and Trade Facilitation February 2003 Meeting, page 1.

- (d) If an RF device, operate within a single radio frequency bandwidth approved and publicly available in all trading nations;¹³
- (e) Must be able to be read by a universal reader capable of interrogating seals from different manufacturers;¹⁴
- (f) Must perform reliably in all operating environments with an insignificant number of false readings; and
- (g) Meet the minimum physical security standards of the ISO high security seal standard.

The container number does not need to be recorded in the device because that will be captured in the shipping documents, and the shipping documents will need to be cross-referenced anyhow by the carrier to ensure that the seal number provided by the shipper for inclusion in the bill of lading is the seal number on the container.

Because its security purpose is to provide evidence regarding whether the seal has been opened or tampered with in transit, an e-seal would only need a “read” capability, not a “read and write” capability. Adding a “write” capability to e-seals could create, rather than reduce, security vulnerabilities, e.g., security credentialing of all persons with “write” capability, the impossibility of monitoring whether unauthorized persons obtained the “write” capability, and potential manipulation or alteration of the data already entered into the device, as well as other cyber-security related vulnerabilities.

¹³ Discussions at the ISO to establish an e-seal standard have not been successful, in part because e-seal manufacturers cannot agree on a single radio frequency (RF). The operational and logistical difficulties of having to try to work with multiple different radio frequencies at the same time, however, are substantial.

First, whatever RF bandwidth is chosen, it is essential that the bandwidth be publicly available in all trading nations. If the bandwidth is available in the U.S., but not, for example, in China, the electronic device’s purpose would be thwarted.

Second, a fundamental characteristic of the liner industry’s operations is the efficient movement of containers through many different facilities and many different national jurisdictions in many different ways. In order to be able to read e-seals on containers in a multiple radio-frequency-environment, the carriers and numerous land-based facilities around the world would have to install different types of readers. Alternatively, the industry would have to invest in multi-frequency seals and readers. Neither of these options would be operationally attractive, cost-effective or in conformity with what should be the objective of any standard setting process -- the development of a common standard and the avoidance of incompatible solutions.

Furthermore, a standard must ensure e-seal *interoperability* amongst all trading nations. Multiple bandwidths may accommodate the desires of various seal vendors that want to use those varying parts of the spectrum for their particular products, but it does not ensure international interoperability. For example, assume that Nation A elects one bandwidth for this use but not others. What effect would that have on operations and the government’s treatment of containers, affixed with seals using the other bandwidths, being shipped to or from Nation A?

¹⁴ Even if all e-seals were to operate at the same frequency, there is still a concern that e-seals are being designed by manufacturers to require proprietary readers. Marine terminals need to be able to use a universal reader capable of interrogating different seals manufactured by various manufacturers.

The commercial availability of such devices and their readers, at reasonable and competitive prices, will be a significant factor to carriers, shippers, and terminal operators in their decision regarding whether to use manual or electronic seals as an indicator of in-transit tampering.

C. Future “Smart Container” Vision

A shipping container is a sturdy steel box. It is not “smart”. A security-marketing vernacular has arisen suggesting that certain technologies might be available that could enhance security, and that this would create a “smart” container of the future. It would be a serious security error simply to assume that technology can be applied to shipping containers and “solve” the problem of container security. It would also be a mistake to think that such a concept can replace enhanced screening and inspection of containers or more secure operating procedures, especially those involving the stuffing of the container.

As unfortunate and misleading as the term “smart” container may be, it would also be a mistake not to assess what technology may be appropriate for containers that would reduce their in-transit security vulnerability and enhance security. The following observations should be relevant to this examination.

1. *Some of what can make a container more secure (and presumably “smarter”) does not involve high technology.*

Container seals have traditionally been applied to the container door handle or door hasp. As drug traffickers have demonstrated, this location for the seal has vulnerabilities, and seal location can be improved. There are a variety of ways this can be addressed, including cable seals, and different locations for the seal. The industry is committed to continue to work with the government to address this vulnerability.

Container doors can often be removed from the outside of the container, leaving the seal intact. The possibility of modifying the design of future containers that will be built to eliminate this risk should, as a matter of priority, be pursued in accordance with the provisions and procedures of the 1972 IMO Convention for Safe Containers, and possibly also the 1972 Customs Convention on Containers.¹⁵ The United States is a signatory to both conventions. Efforts are

¹⁵ The 1972 Customs Convention on Containers provides for the incorporation of such design features for containers moving under Customs seals. Those provisions have hitherto not been utilized. The governing body of the Convention will meet in late October to discuss, inter alia, the possibility of activating those provisions. In such an event, the ISO could be expected to be called upon to develop specific standards for new design features.

underway at the ISO to ensure that the necessary standardization measures can be taken to accommodate future design modifications.¹⁶

The required application of a high security seal by the shipper upon stuffing the container will make it more secure, and this should be required as a matter of law – preferably by a mandatory, international instrument.

2. Some of what is promoted to make a container “smart” has no security foundation, and in fact could create security problems.

For example, an electronic tag can be affixed to the exterior of the container and contain the shipper’s description of the cargo. While some vendors have stated that this is a way to enhance security by telling someone with a reader what is in the box, this is not correct. First, such a tag only provides the information that the party filling out the cargo declaration records in the device. Secondly, this could increase security risks of theft, as anyone with a functioning reader could know the contents. There are also unsolved cyber-security issues, including the risk of manipulating the stored information to disguise the true nature of the contents. Third, the carrier and CBP already have the shipper’s cargo description in the carrier’s cargo manifest, and CBP already performs its security screening based on this manifest information which is provided by the carrier to the government 24 hours before the container is loaded aboard a vessel.

For example, some parties describe “smart” electronic devices as having both the ability to be electronically “read” for certain security information (such as whether the seal is the same seal that was applied by the shipper upon stuffing the box and whether it is intact), and having the ability for people to “write” information into the device. We do not see “write” technology as a security need or enhancement, and in fact, believe it can create significant security vulnerabilities and complexities.¹⁷

3. A security technology and security function of very high importance is non-intrusive container inspection equipment, which is not part of the container.

We strongly believe that CBP’s container risk assessment programs and their implementation (via inspection of any container that does not meet risk analysis criteria) should be enhanced so that any questions about a container’s contents are addressed by non-intrusive inspection of the container, preferably at the port of loading pursuant to bilateral or regional CSI-like agreements rather than at the port of discharge. We believe that continued enhancement of non-intrusive container inspection equipment availability and technology is critically important, as it answers the question of most importance and relevance, namely:

¹⁶ The ISO has traditionally played a supporting role for the IMO Convention and changes to it. Thus it is appropriate that the ISO prepare itself for future design decisions of the IMO and their practical implementation.

¹⁷ See Part B above.

“What is in the box?” No container can be “smart” enough to answer that question.

This is an important point that should be emphasized. Non-intrusive container inspection equipment is necessary as a preventative mechanism to enhance security, and just as importantly, it is likely to be one of the most important tools available to confidently keep international trade flowing in the event of a terrorist crisis. That is one of the reasons the CSI program is so important to international trade, and why all CSI countries need to have sufficient non-intrusive container inspection equipment to address both prevention and response scenario needs. While the U.S. government is considerably expanding its equipment availability in this regard, it is just as important that such equipment also be properly deployed in adequate quantities at foreign ports of loading.

4. Technology to detect radiation or various different kinds of chemicals or substances emanating from particular kinds of cargo in a container should be deployed by government inspectors at ports, not applied to approximately eleven million containers in circulation around the world, which pass through the possession of numerous parties who would have the opportunity to tamper with or disable the detector or sensor.

There are many questions regarding the concept of requiring containers to be equipped with various possible sensors, rather than having such sensors used by government law enforcement officials inspecting containers.

First, it is unclear what specifically would need to be “sensed”; the list of potential substances or characteristics is long, varied, not agreed and imprecise. Second, it is very unclear what the operational reliability of such sensors would be when deployed on containers that travel considerable distances, through many operating conditions, and for long periods of time without servicing internal electronic devices. Third, the government is already working on and deploying inspection sensors and detectors for nuclear, radiological, drugs and other substance sensing that can be more effectively and efficiently deployed via inspection of the container at the port rather than via attaching multiple electronic sensor components to eleven million containers. Fourth, a future vision in this context should be one that could realistically be *years* away, not *decades*. Even if the devices were available to be installed in or on containers at reasonable cost, did not provide false positives, were maintenance free, were reliable, and were tamper-proof, it would be far more efficient and reliable for the government to operate and deploy them at inspection points and ports. That capability could be deployed relatively quickly and efficiently in contrast to the enormous difficulty in trying to retrofit such devices onto more than eleven million containers that are located all around the globe. Fifth, even if such sensors could be applied to containers, there are types of containers on which they would be completely ineffective, such as open tops and flat racks. Port based sensors and non-intrusive inspection equipment is the only way to effectively

address security concerns about these kinds of shipments. Finally, outfitting millions of containers with one or more electronic devices would raise very substantial information system issues, which are discussed under Item 6 below.

5. *Some technology features discussed as part of a “smart” container are not practical security features.*

For example, some have suggested every container should be electronically programmed with a trip plan for each shipment, with a requirement or expectation that any shipment that deviates from the trip plan be identified and subjected to security scrutiny. This would raise a host of issues, including subjective determinations of reasonable deviations and a plethora of false security alerts that would destroy the credibility of the device.

For example, some have suggested “smart” containers or “smart” container equipment be electronically tied to the security credentialing of each person who seals and loads a container. Personnel credentialing may be appropriate for a shipper as part of C-TPAT or similar risk assessment programs, but not as part of a container. It would create far too many complexities. Furthermore, the electronic device on the container would also be easily fooled or defeated by an even moderately sophisticated conspiracy.

6. *There are, however, container security attributes which technology may be able to address more effectively and which the industry would like to consider in concert with the government.*

A. **Intrusion**: The first attribute that falls into this category is the detection of container *intrusion*.

First, it is important to obtain agreement on this term’s definition. For example, we believe the term “intrusion” means intrusion into the container from any exterior location, i.e., floor, walls, roof, doors. Seals and e-seals detect tampering with a seal, but not container intrusion -- despite some manufacturers’ marketing claims. Some other devices may be able to detect if the container doors have been opened, but not if the container was entered through the roof. Agreement on the definition is thus quite important.

Second, such technology must be reliable, must be low maintenance, must provide an insignificant number of false alarms, and must be reasonably priced. The technology must not be something that can be disabled. This technology would need to be fully and satisfactorily tested in a commercial operating environment that involves the government, carriers, shippers and other parties with possession of the containers.

Third, consideration must be given to what kind of technology can meet a requirement to detect intrusion. Must it be electronic? If it is, how will its information be communicated? Through readers at specific locations?

Fourth, there are very complicated information and accountability questions that must be addressed in considering this issue. Whose information system obtains the information? Who acts on the information? How does one screen the many benign intrusions (e.g., door opening by a Customs inspector) from non-benign intrusions, and who would do the screening, evaluation and action assessment? Consider an example -- an ocean carrier may move a container on a port-to-port bill of lading, completing its service at the port of discharge. Assume that a trucker at the shipper's direction then picks up the container at the port and transports the container under its own, separate bill of lading, and during that service by the trucker, there is an intrusion. Who is alerted? Who determines if there is a security issue? Who resolves it? Consider another example -- a carrier agrees with a third party transportation broker to reposition its empty container from the East Coast to a West Coast port. Assume the broker uses the container for the movement of cargo for one of its customers to the West Coast, as frequently occurs, and during that movement, there is an intrusion. Same questions as above.

It is also very important to understand that an ocean carrier does not have physical custody of its containers most of the time. We estimate that, on average, ocean carriers have custody of their containers roughly 25 to 33 percent of the time. This number can be more and can be less depending on the geographic trade lane that the equipment may be in at the time, or the equipment operating practices of the carrier. The rest of the time, the container will not be aboard a vessel or in a port but may be in the possession of a number of different parties, such as a railroad, a trucker, a barge company, a consolidator, a warehouse, a shipper, a shipper's supplier, or a consignee. Furthermore, containers may be interchanged between or among different shipping lines, meaning Line A's container could be full of cargo being transported by Line B. Furthermore, containers do not operate in dedicated service to and from the U.S., but are elements of global container fleets and used to move cargo globally. A container that moves goods in U.S. foreign commerce today may not ever come back to the U.S.

Accordingly, intrusion technology would require the above issues to be considered and addressed, including the information and accountability issues when the ocean carrier does not have possession of the container. And, technology permanently affixed to a container would not be practical if it were only for U.S. commerce and did not meet internationally agreed standards.

In sum, the industry believes that container intrusion detection may be an appropriate objective to explore, but it will require considerable analysis in order to address legitimate and complicated issues.

B. **Location**: The second security attribute that may fall into this category is container *location*. The security interest involved is to be able to quickly locate a container that may be identified as containing a potential security risk.

Carriers already have significant container location capability. If the container is on a vessel, the carrier will know the vessel's position and the position of the container on the vessel. If the container is at a marine terminal, the carrier can contact the marine terminal directly or through the terminal operator's information system to determine the location of the container in the yard. If the container is on a train, the rail carrier will know the location of the train and the location of the container on the train. If the container is with a trucker, the ocean carrier will know who the trucker is. Some trucks have GPS capability in North America, but not all.

It is true that this container location capability relies on databases and their accessibility, rather than real time location capability. But this only illustrates that container location, or, more precisely, the ability to locate a container within a relatively short, defined time frame requires a careful and specific discussion of what this requirement would be. The technology involved could vary substantially depending on the definition of the requirement. For example, how precise a location would be required? Does this envision the capability to locate a container only in the U.S.? On a ship, stowed below deck? On a ship anywhere in the world? In container stacks in a terminal, aboard a barge, a double-stack train, etc? Anywhere in the world? Also, discussion and agreement would be needed on the issue of how quickly the container would need to be located. The technology, its cost, and its practicality could vary significantly depending on the definition of the requirement.

Also, if this objective were to be addressed through an electronic device, the issues identified in Item 6A. regarding information systems and accountability issues would have to be addressed. In addition, any such device would have to be incapable of being disabled if it is to accomplish its presumed security purpose.

D. Conclusion

Enhancing the security of international commerce is a shared responsibility of shippers, transport providers, ports and marine terminals, and governments. The clear definition of parties' roles and responsibilities, backed by uniformly applied government regulatory requirements, is essential.

This paper offers a proposed set of concepts and requirements from the liner shipping industry and shippers to address in-transit container security. The industry recognizes that in-transit container security, while not the principal

security vulnerability of such commerce, should be governed by predictable, transparent and consistent rules addressing the issue.

Part A of the paper offers a proposed vision for specific, actionable measures to enhance the in-transit security of containers. The paper proposes that these measures be implemented as government requirements. Why is the industry asking for government requirements to do this? There are a number of reasons. First, these security measures both are expensive and will at times inconvenience commerce. If one company inconveniences its customers or must incur substantial costs, but the competition is not doing the same thing, the security measures are unlikely to be effectively implemented and compliance will be inadequate. All parties must be required to play by the same rules and be on a level playing field. Second, if the measure provides a valid enhancement of security, everyone should be required to do it. Third, the industry wants to be sure that the proposed measures meet, conform with, and reflect the government's requirements and objectives on this issue.

Part B of the paper offers ocean carriers' and shippers' views on the potential use, value and features of electronic seals. There is still considerable uncertainty about the capabilities, operability, reliability and costs of such devices, as is discussed in the paper. Electronic seals are not capable of being adopted in a commercial context in the short run; however, members of the industry want the ability to consider whether they can meet seal checking requirements more efficiently and effectively by electing to use such technology. For that reason, the industry has identified what it believes are the necessary and appropriate security requirements of an electronic seal. The development and deployment of e-seals will only be delayed by product vendors trying to add features to the devices that are not necessary for meeting security objectives, and by the failure to adopt a single, universally available radio frequency bandwidth. The industry hopes that an articulation of what the devices' security requirements should be will help focus and progress the discussion of this issue.

Part C of the paper offers industry comments on how future technology may be applied to enhance the security of international commerce, and when such technology would be most effectively applied at inspection points rather than affixed to eleven million instrumentalities of international commerce. In this part, the industry stresses the priority need for the improvement and expanded deployment of non-intrusive container inspection equipment. The CSI infrastructure being constructed to enhance security requires a clear focus on making sure that this technology is properly deployed and used, not only at U.S. ports of discharge, but at ports of loading around the world.

The Council, IMRA, the League and their member companies remain committed to continued close cooperation with the government on the wide range of security initiatives – including vessel security, port facility security, personnel security, container stuffing security, and container screening and inspection. The Council, IMRA, and the League hope that this paper is a

constructive contribution to that effort, and are willing to present and discuss these issues in greater detail to all relevant government agencies, including how these issues can also be addressed and pursued at the international level.

The World Shipping Council, a non-profit association of over forty international ocean carriers, was 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 more than 93% of the United States' imports and exports transported by the international liner shipping industry, or roughly \$500 billion worth of American foreign commerce per year.

The International Mass Retail Association is the world's leading alliance of retailers and their product and service suppliers. IMRA members represent over \$1 trillion in sales annually and operate over 100,000 stores, manufacturing facilities, and distribution centers nationwide. Our member retailers and suppliers have facilities in all 50 states, as well as internationally, and employ millions of Americans. As a full-service trade association, IMRA provides industry research and education, government advocacy, and a unique forum for its members to establish relationships, solve problems, and work together for the benefit of the consumer and the mass retail industry.

The National Industrial Transportation League is an organization of shippers that conduct industrial and/or commercial enterprises throughout the United States and internationally. The League, founded in 1907, is the oldest and largest U.S. organization representing shippers of all sizes and all commodities. The League has approximately 600 separate company members. These include some of the largest commercial and industrial enterprises in the United States, many with operations throughout the world, as well as numerous smaller shippers. League members ship substantial volumes of commodities worldwide in all major international trades via ocean carriage.