

Departmental Advisory Committee on Commercial Operations of Customs & Border Protection (COAC)

Maritime Transportation Security Act Subcommittee Recommendations to COAC and the U.S. Department of Homeland Security

Deliverable #1: Short Term Minimum In- Transit Container Security Enhancement

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 physical 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, and this proposal makes the assumption that all parties throughout the supply chain recognize and accept that 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 proposal assumes that the ocean ports of lading and unloading are ISPS secured facilities. In addition, the proposal assumes that government

information systems, such as AMS, will continue to support the data elements needed to sustain these security enhancements.

This proposal, 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 proposal only addresses the issues 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 Part I of the MTSA Subcommittee recommendations addresses what can be done in the short term to enhance the in-transit security of loaded containers being shipped to the United States.¹ By "short term", we mean within 12 months.

The security regime proposed below would not apply to empty containers. The MTSA Subcommittee recognized that the shipment of empty containers may also represent a different set of issues for security concerns and formed a Working Group on Empty Container Security to explore these issues in greater detail. The MTSA Subcommittee recommendations on securing empty containers are set forth in Part II of this document.²

¹ 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 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.

² The ILWU did not agree with the Subcommittee recommendations on Empty Container Security.

A. Proposed Short Term Vision

Based on the foregoing, and recognizing the past work of the Container Working Group and other entities, as well as requirements of the Customs-Trade Partnership Against Terrorism (C-TPAT), we propose that the government establish the following requirements:

1. **Obligation To Seal**: The party that physically performs the safe and secure loading or “stuffing” of the container is responsible for sealing the container immediately upon the conclusion of the safe and secure stuffing process. The shipper must provide the seal number to the carrier.
2. **Seal Standards**: All seals should meet the ISO standard for high security seals (PAS 17712)³. We recommend that the government establish a specific date by which all containerized shipments must be affixed with such seals by the party that physically performs the safe and secure loading or “stuffing” of the container. If that party chooses, it may use a seal that exceeds the minimum standard.
3. **Recording Seal Changes**: When persons having custody⁴ of a container, including U.S., state and local government officials, break the seal for legitimate reasons, they must affix a new seal meeting the ISO standard, and immediately provide the carrier (*e.g.*, trucker, railroad, ocean carrier) or terminal operator in possession of the container with written or electronic confirmation⁵ of the event. The carrier must record the new seal number on the relevant shipping documents.⁶

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. We recommend that CBP work to incorporate this requirement into the various Container

³ We note that a seal does not need to be a “bolt” seal to comply with this standard, and that cable seals can comply. Question 9 in the May 10, 2004 “DRAFT Proposal for the Implementation of Requirements under the Maritime Transportation Security Act (MTSA),” which was prepared by the Department of Homeland Security (DHS), could be interpreted to imply that only bolt seals comply.

⁴ In this context, persons with “custody” have a right to inspect or gain access to the contents of the container during transit. Such persons might include, in addition to the party with physical possession of the container, the government officials referenced in the text, persons such as hazardous materials incident first responders, insurance inspectors, or representatives of the cargo owners.

⁵ An example of an acceptable electronic communication would be an e-mail or EDI message that contains the new seal number.

⁶ As used in this document, the term “shipping documents” includes bills of lading, waybills and any other transportation document associated with a carrier’s transportation of the shipment.

Security Initiative (CSI) agreements with other governments. In this regard, it is important to recognize that there are seal changes on hundreds of thousands of container shipments in U.S. commerce each year, and that the vast majority of them would not give rise to security concerns. For example, in some countries, local Customs may break the seal on every export container and affix a new seal. Other locals (principalities, etc.) have the right to break a seal. No common practice or approach exists today internationally for the written or electronic confirmation of such occurrences or for the kinds of seals that should be affixed after the original seals have been broken by local Customs.

4. Modal Changes: Ideally, at each modal interchange⁷ in custody, the party receiving the container (*e.g.*, trucker, railroad) 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.

Recognizing for the purposes of the MTSA Subcommittee that the U.S. government cannot legally require truck and rail operators in foreign jurisdictions to perform a particular action, we recommend that the government requirement for import cargo be that an ocean carrier (or its agent) transporting a loaded container to the U.S. be required to perform the verification procedure outlined in Section 6 below.

It is important to note that these recommendations do not yet address what a motor carrier or railroad would do if they discovered an anomaly during a modal change inspection. Some inspections are for commercial rather than security purposes and should not be mandated under the aegis of security. In addition, the intent of the Subcommittee is to be neutral on collective bargaining issues, specifically as to who performs the inspections.

5. Seal Placement: DHS' May 10 Draft Paper to the MTSA Subcommittee proposes to require: "Seal placement in a manner that precludes circumvention by removing door hinges, latches, hasps, or other container hardware, without evidence of tampering". The Subcommittee recommends that any ultimate requirements for equipment modifications be handled on an international basis to maintain maximum utilization of the entire container population.

⁷ "Modal interchange" in this context refers to 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 stack train is transferred from one railroad to another railroad.

We note that no seal placement can preclude removal of container door hinges. The Subcommittee also is mindful of the fact that tampering can occur in other ways, and recognizes that DHS is examining this issue.

It is also our understanding that the 1972 Customs Convention on Containers provides that signatory nations, including the United States, must admit a container that is found by another signatory to be compliant with the convention. Thus, a container owner cannot be required to modify its equipment for it to be permitted entry under the terms of the 1972 Convention and other related international instruments.

Furthermore, it is essential that DHS clearly define what manners of seal placement would meet with this objective. Our understanding is that CBP has identified the following alternatives as “acceptable”:

- Properly applied cable seals⁸
- Seal applied in the “SecuraCam” location
- Seal applied in the P&O Nedlloyd-developed “Locking Rod Seal Retainer”
- Seal applied in a “Pardo Hole”⁹

In addition to the above, it is important that CBP/DHS establish a process whereby additional alternatives to the above can be reviewed and, if determined adequate, approved as acceptable, and that fact made publicly known on CBP’s website.

DHS will investigate the application of the 1972 convention to equipment modifications to determine if there are provisions allowing alterations for national security purposes. The Subcommittee also asks that DHS differentiate sealing from physical equipment modification.

6. Ocean Carrier Seal Verification: DHS should by regulation require the ocean carrier or its agent to verify the applied container seal before loading a container onto a vessel bound for the U.S. by determining:

- (a) Whether a proper ISO standard seal is affixed to the container¹⁰,
- (b) If in the affirmative, whether the seal is intact or exhibits evidence of tampering,
- (c) What the seal number is, and
- (d) Whether that seal number is the same as stated by the shipper was originally affixed to the container.¹¹

⁸ CBP’s description of “properly applied” cable seals can be found at: http://www.cbp.gov/ImageCache/cgov/content/import/commercial_5fenforcement/ctpat/fast/fast_5fconveyance_5fseals_2edoc/v2/fast_5fconveyance_5fseals.doc

⁹ We note that CBP/DHS to date has provided no engineering specifications for a “Pardo Hole.”

¹⁰ See footnote 19 below.

The verification for ISPS-compliant facilities 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 have inadequate security, then CBP, in consultation and coordination with the U.S. Coast Guard which has regulatory responsibilities for foreign port assessments, should include this shortcoming in its Automated Targeting System (ATS) to determine the appropriate oversight 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.¹²

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

A majority of the Subcommittee believes there is no need to check the seal upon discharge from the vessel in the U.S. The seal will be verified by the U.S. modal operator moving the box to its inland destination as described in Section 4 above. [33 CFR 105265]¹³

¹¹ There will be 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 CBP determines that 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.

In addition, functionality in ACE will be needed to transfer the seal numbers from one mode to another. While this can be accomplished in the rail mode at present, a transition period may be necessary for the trucking industry.

¹² These procedures could be included in the vessel carrier's security plan developed in accordance with its C-TPAT membership status.

¹³ See Part II for discussion of empty containers; the ILWU did not agree with the recommendations.

7. Addressing Seal Anomalies: There are four different kinds of seal “anomalies” that could arise under the above proposal: 1) seal does not meet the ISO standard, 2) seal number does not match the seal number in the shipping documents, 3) seal has been tampered with and is not intact, or 4) the seal is missing. The following is a recommendation for how these situations could be addressed:

- a) If an ocean 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 the shipper and CBP of the fact in its AMS filing. CBP should consider such information in its ATS profiling of container shipments.¹⁴
- b) If during seal verification, the ocean carrier finds that the seal on a container is broken, missing, or has been tampered with or finds that the seal number does not conform to the seal number in the shipping documents, the carrier shall immediately notify the shipper and CBP of that fact.¹⁵ Members of the Subcommittee reached consensus (with one member abstaining) that, unless instructed by the shipper or CBP not to load the container onboard prior to vessel loading, the carrier will properly apply a conforming seal to containers with missing or broken seals, load the container, and allow CBP to address the issue at the U.S. discharge port. Two other options also were considered but were viewed as less feasible: (1) the carrier shall not load the container until the importer instructs the carrier that the issue has been investigated, and it is okay to load; and (2) the carrier shall not load the container until CBP informs the carrier that it is okay to load the container.¹⁶

The Subcommittee requests that – before any seal verification requirements become effective – CBP program AMS to accommodate notification of such seal anomalies. CBP should provide a clear

¹⁴ We believe that it is important for CBP to establish significant consequences for cargo interests if shippers 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.

¹⁵ As noted in footnote 11, verification of seal numbers under current operating procedures may not always identify an anomaly until after vessel loading for cargo arriving at the marine terminal just before vessel loading. If the government wants to require the carrier to verify the seal number before vessel loading, it needs to clearly state that as a requirement. This could require earlier cut-off times and delay some commerce.

¹⁶ The industry has considered but does not prefer this second option because there will be a substantial number of seal anomalies identified, and most have acceptable explanations and are not a security risk. CBP retains the ability to inspect a container with a seal anomaly at the U.S. port of discharge.

protocol for what the government will do with this information, which should be linked to ATS. CPB may order the inspection of any container that has had a seal anomaly.¹⁷

B. Implementation Timetable

The above recommendations should be implemented throughout the supply chain by mandatory regulations. We recommend that implementation be within 12 months, but no earlier than within six months of the issuance of final regulations. This should provide sufficient time both to promulgate and finalize a rulemaking and to communicate and prepare shippers, carriers, agents, terminal operators and customs authorities around the world for changes to their processes.

In the meantime, an essential voluntary aspect of this initiative would be increased vigilance on the part of all entities involved in international freight movements.

C. Answers to DHS Questions Posed in Draft Paper

1. Q: Is the ISO / PAS 17712 an acceptable minimum standard to provide immediate enhancements to the physical security of containers transported through supply chains with a maritime nexus?

A: Yes.

2. Q: What additional security practices and procedures would be viable to address container security in the short term?

A: See recommendation above.

3. Q: Who should be responsible for the application and verification of container seals throughout the supply chain?

A: The party loading the container is responsible for the safe and secure loading of the cargo, for properly affixing a compliant high security seal, and for properly recording the seal number on the shipping

¹⁷ 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, significant delays to commerce, and increased congestion at foreign marine terminals. As noted in footnote 12 and this footnote, the recommended reporting of seal anomalies is not tied to the reporting time frame or requirements of the 24-hour rule – *i.e.*, it is not, in and of itself, a factor triggering a delay in lading.

documentation. Each modal carrier that receives the container is responsible for verification of the seal upon taking receipt of the container.

4. Q: Should the implementation of minimum standards for the physical security of a container be a part of a voluntary, incentive-based program or should it be mandatory requirement?

A: By definition a “minimum” standard must be a mandatory requirement, or it is not a minimum. Some such standards are currently voluntary under C-TPAT and an interim phase-in period would be needed as the voluntary requirements of existing programs are replaced with mandatory standards. Voluntary, incentive based programs may be appropriate for security enhancement measures that go beyond the minimum. Thus, certain “smart” container technologies might be appropriately considered for implementation through a voluntary, incentive-based program. If implemented, CBP should factor that into its ATS system.

5. & 6. Q: Significant consideration has been given to improving the physical security of empty containers. The CWG recommends that all empty containers destined for the United States be inspected and certified as empty by the carriers or their trusted agents (CWG Report, April 2002). Vessels and marine terminals that participate in C-TPAT also have agreed to inspect all empty containers prior to loading them aboard a vessel, and to ensure empty containers are stored in a secure manner while at the terminal. Are there other options DHS should consider for increasing the security of empty containers?

A: The Subcommittee recognizes that empty containers may represent a security concern and has formed a Working Group on Empty Container Security to investigate and make recommendations on securing empty containers, as appropriate.¹⁸

7. Q: Do you agree that the phased approach to establish security standards is appropriate and do you agree that the progression of those proposed standards (*i.e.*, short-term, mid-term, long-term) is reasonable? How would you define short-term, mid-term and long-term?

A: Yes. Short term is defined above as 12 months for full global implementation. It should be noted, however, that the issuance of DHS’ “gap analysis” in the near future may result in some revisions to the Subcommittee’s position on issues discussed within.

¹⁸ The consensus recommendations (ILWU not agreeing) from the Working Group on Empty Container Security are included in the package of documents submitted by the MTSA Subcommittee to COAC pertaining to Deliverable # 1.

8. Q: What is the earliest date that industry could comply with for the proposed short-term minimum-security standards for high security seals in an alternate location on intermodal containers and accompanying seal protocols?

A: We believe 12 months is an appropriate time for an orderly compliance. There are many variables that have to be addressed in complying with the above recommendations. Should the alternative seal placement be made a requirement, a very substantial portion of the existing container fleet would either have to be physically modified or the shippers would have to use cable seals in a specified manner. Furthermore, for the change to have meaning, verification appears necessary. Verification procedures and accountabilities, including those involving the government, must be agreed to and specified; implementation procedures must be developed by shippers, consignees and carriers and their agents; the new procedures must be communicated to thousands of shippers around the world; the new procedures and operating protocols must be communicated by CBP to its counterparts in the rest of the world, particularly in CSI ports.¹⁹ Given these factors, the Subcommittee might propose a phase-in of requirements as positions mature.

9. Q: What are the operational and accompanying economic impacts for the use of high security bolts seals in an alternate location and accompanying seal protocols?

A: First, as noted in footnote 3, the ISO high security seal standard does not require the seal to be a bolt seal. Second, the additional cost of an ISO compliant high security manual seal is reasonable, as a compliant bolt seal costs \$ 0.40-0.50, whereas prices for compliant cable seals start around \$2. Third, the cost of retrofitting containers, via addition of a SecuraCam, the PONL locking rod seal retainer, a Pardo hole, or other mechanism would be very substantial. There are roughly 17 million containers in the global container fleet. They do not operate in closed or dedicated loops, but are deployed in the most efficient manner, meaning that any container must be able to be deployed in U.S. trades, meaning that, if compliance were through retrofitting containers with new physical features, the cost would be in the many hundreds of millions of dollars. If compliance would be achieved by the general application of cable seals to the legacy container fleet rather than physical modification, the cost to trade would be significantly less.

¹⁹ The current version of ISO PAS 17712 does not require any visual identification to be printed/stamped on the seal to indicate that it is a “high security” PAS 17712 compliant seal. Future versions of PAS 17712 should include such a requirement in order to facilitate the proposed seal verification procedures. Until such a clear external manifestation of this nature is required to be on the seal in order for it to be compliant, a verifying party should not be held accountable if a seal appears to be compliant but is not.

Finally, as noted earlier, we understand that the 1972 Customs Convention on Containers provides that signatory nations, including the United States, must admit a container that is found by another signatory to be compliant with the convention. Thus, a container owner cannot be required to modify its equipment for it to be permitted entry under the terms of the 1972 Convention and other related international instruments. Clearly, other means exist to implement the government's security objective when it is defined (*e.g.*, a shipment will be subject to a large-scale non-intrusive inspection). However, the 1972 convention illustrates that there is a need to recognize that this is international commerce that needs both workable and internationally understood rules, and the U.S. government should therefore consider raising these issues in the appropriate international fora.

10. Q: What are the operational and economic impacts of inspecting empty containers prior to loading on a vessel?

A: Operational protocols and thus costs for the inspection of empty containers at receiving marine terminals prior to vessel loading vary throughout the world, based on what is practicable for each location. It is therefore not possible to provide a more detailed description of the operational and economic implications of such inspections.

11. Q: For the short-term, do you have other recommendations to increase the security of intermodal containers that are transported through a supply chain with a maritime nexus?

A: Ocean carriers and terminal operators are currently working to implement the ISPS Code security enhancements for their ships and marine terminals. This is a substantial effort and one that will increase security.

We strongly support and encourage further implementation and development of the Container Security Initiative, so that U.S. and foreign customs authorities can expand their cooperation, and improve their information sharing and targeting of high risk shipments.

We support the development of clear criteria for C-TPAT and/or "green lane" treatment that more effectively address the secure stuffing of containers at origin.

We recommend clarification of modal responsibilities with respect to seal verification.

MTSA Subcommittee Recommendations to COAC.

Finally, we believe that a critically important way to improve the security of legitimate trade moving in America's supply chains is to continue to enhance the Automated Targeting System's ability to better identify those container shipments that could put the vessels, ports and compliance of legitimate cargo at risk.

Deliverable #1: MTSA Subcommittee Recommendation Regarding Empty Containers

The MTSA Subcommittee approved the following report and recommendation of a special MTSA Subgroup that was created to consider the issue of empty containers.

DHS officials began the meeting by explaining that there is a Departmental consensus that empty containers do not present a sufficient security risk to require container sealing. DHS officials stated that sealing an empty could in fact make checking the conveyance more difficult. There was a discussion and recognition that in certain situations, based on specific risk assessment (such as in the SuperCarrier agreements in Central American trades), sealing empties might be appropriate.

Recognizing that there was not a basis for requiring the sealing of empty containers, the Subgroup then considered the issue of whether empty containers should be inspected. At the conclusion of considerable discussion of the issue and a recognition that no meaningful government threat assessment exists to guide industry discussion on this issue,²⁰ the Subgroup reached consensus (ILWU not agreeing) as follows:

1) For inbound (i.e., U.S. import) empty containers arriving at a U.S. port on a vessel from a foreign port, ocean carriers had recognized CBP's admittedly very general risk assessment that inbound empties presented a potential security risk and thus have agreed in their Sea-Carrier C-TPAT Agreements with CBP to "visually inspect all empty containers, to include the interior of the container, at foreign ports of lading". It was recognized that close to all arriving containers are carried by C-TPAT carriers, but CBP was asked to determine: (a) what percent of empty containers arriving at a U.S. port from foreign ports are carried by carriers that are not C-TPAT carriers, and (b) to provide the Subcommittee with the total number of empty containers arriving in U.S. ports from foreign ports. In

²⁰ DHS subsequently confirmed that their intelligence analysts indicate that there is little analysis on empty containers.

this regard, CBP was asked to make sure that in determining this latter number that empty containers being unloaded from a vessel at a U.S. port that had been loaded aboard at another U.S. port were not included in the calculation. CBP responded by informing the Subgroup that C-TPAT Sea Carriers account for 96 percent of containers arriving in the U.S., and that there are approximately 300,000 empty containers that arrive empty. While there was discussion that the threat assessment used by CBP in considering empty container treatment in C-TPAT was exceedingly general, and that a random inspection percentage might be preferable, the consensus of the Subgroup was that the current C-TPAT approach to inbound empty containers was acceptable and did not need to be changed.

2) For inbound empty containers arriving at a U.S. port, the Subgroup agreed that an empty that has been inspected at a foreign port of loading does not need to be re-inspected at the U.S. port of discharge. Coast Guard and CBP officials in attendance concurred that this was the government's view.

3) For outbound (i.e., U.S. export) empty containers arriving at a U.S. port facility, there was discussion of the lack of a threat assessment, the complexity of the issue if empty vehicles utilized in domestic transportation are perceived to present a significant terrorist threat, and the substantial costs and operational issues that would result if every outbound container received at a U.S. port were required to be inspected. The consensus of the Subgroup was that a security analysis should be conducted to ascertain the existence, nature and magnitude of a potential threat of terrorists using empty containers, and that this analysis should consider the life cycle of the container from the time it is emptied of cargo until it is either reloaded with cargo or exported. Notwithstanding the current lack of a threat analysis on this question, the MTSA Subcommittee recommends that for outbound empty containers the issue should be addressed under the Coast Guard's MTSA regulations by having the receiving port facility, pursuant to its approved facility security plan, randomly screen arriving empty containers to verify that they are empty at the same rate that the facility screens cargo transportation vehicles entering the facility pursuant to its facility security plan. The facility could use technology to meet this objective.

Deliverable #2: Secure Systems of Intermodal Transportation

The Department of Homeland Security, under the direction of the Border and Transportation Security Directorate, has established the MTSA Subcommittee for the purpose of reviewing what additional measures should be taken to fulfill the requirements of the MTSA to establish “secure systems of international intermodal transportation”. Specifically, the Act requires the Department to:

“Develop and maintain an antiterrorism cargo identification, tracking and screening system for containerized cargo shipped to and from the United States” (Section 111(1)).

“Develop performance standards to enhance the physical security of shipping containers, including standards for seals and locks” (Section 111(2))

Establish “a program to evaluate and certify secure systems of international intermodal transportation”, (Section 70116(a)) which shall include:

- “establishing standards and procedures for screening and evaluating cargo prior to loading in a foreign port for shipment to the United States”; (46 U.S.C. 70116(b)(1))
- “establishing standards and procedures for securing cargo and monitoring that security while in transit”; (46 U.S.C 70116(b)(2))
- “developing performance standards to enhance the physical security of shipping containers, including standards for seals and locks”; (46 U.S.C. 70116(b)(3))
- “establishing standards and procedures for allowing the United States government to ensure and validate compliance with this program”; (46 U.S.C. 70116(b)(4)); and
- “any other measures the Secretary considers necessary to ensure the security and integrity of international intermodal transport movements.” (46 U.S.C. 70116(5)).

The following is a recommendation for the MTSA Subcommittee’s consideration identifying the elements of what should comprise a “secure system of international intermodal transportation”, as called for by the Act. These elements are provided in a logical, but not necessarily prioritized, order.

1) An effective cargo security risk assessment screening system.

This will require obtaining more complete cargo shipment data than is used today; i.e., enhance the Automated Targeting System. The government increasingly acknowledges that the existing targeting data is not adequate.

There needs to be a “blueprint” developed identifying what additional data should be obtained, from whom, when.

- 2) *Effective security cooperation and coordination between governments***, i.e., the Container Security Initiative. This program is essential. There is no international regulatory entity, like the IMO for ships, to establish cargo security rules or screening and inspection protocols. CSI needs to move beyond its developmental stage and be made more robust. At the same time, CSI’s role must be clearly understood. For example, it is convenient, but presumably not correct, for the government to say that in the event of a security crisis, we will only allow commerce to come to the U.S. via a CSI port – as that would suspend trade with Australia, New Zealand, and all of Latin America. In fact, those CSI ports that are operational today account for approximately 40% of the United States’ total containerized imports.

A secure system of transportation that screens and detects security issues before vessel loading requires effective international cooperative agreements. U.S. Customs and the governments of our trading partners should strengthen the Container Security Initiative infrastructure and agree on procedures for security screening and inspection of cargo. CSI ports must not only become operational, but the implementing governments must discuss, understand and agree upon what each other will expect and require of each other. CSI is an important component of compliance with MTSA secure systems of transportation, particularly in that it establishes “procedures for allowing the United States government to ensure and validate compliance” with programs designed “for screening and evaluating cargo prior to loading in a foreign port”. (46 U.S.C. 70116(b)(4)).

- 3) *Transparent, measurable requirements defining a “secure” shipment entitled to “green lane” treatment.***

The Department, in consultation with industry, should establish clear, transparent criteria that the industry and government can understand and plan on for what is required for containerized cargo to be considered low-risk or “secure” and entitled to expedited or “green lane” treatment, including if and when there is a security incident involving containerized cargo. The critical importance of the container stuffing process should be addressed in such criteria. This would also facilitate meaningful contingency planning.

- 4) *Effective contingency planning for how the U.S. government would keep the nation’s foreign commerce flowing in the event of a terrorist attack on or using a container.*** This is a most serious issue. If there is a plan for how this would be done, industry is unaware of, and thus probably unprepared for, what would be expected of it in order to continue transporting America’s commerce. Addressing this admittedly

difficult issue in a coherent and disciplined manner would offer the opportunity to not only create the ability to reduce economic damage to the American economy and global trading system, but address many of the problems outlined above – because it would force the government and industry to address important questions such as:

- What criteria will be used to determine what American trade will be allowed to be transported in the event of a security incident
- What will the U.S. expect and require of foreign governments,
- What will be expected of carriers and marine terminals,
- What will be expected of shippers,
- What will we expect of CBP and what is its role,
- What will we expect of the Coast Guard and what is its role,
- Who will make what decisions, and
- How will that be communicated?

1. Proposed Objective #1: Enhance ATS in Order to Provide More Effective Security Screening of All Containers Before Loading Aboard Vessel

CBP established the “24 Hour Rule” under which the government obtains carriers’ manifest information about all containerized cargo shipments before vessel loading in a foreign port, and then screens the shipment in the Automated Targeting System (ATS) to determine what containers require further review or inspection. We fully support this rule and strategy. This is the correct time and place for the cargo security screening, and ATS would logically be an essential part of the government’s ability to have a coherent, workable mechanism to keep containerized cargo flowing in the event of a security incident.

The government has significantly increased the numbers of containers it physically inspects, but physically inspecting every container has been determined to be both impractical and unnecessary²¹. Notwithstanding statements by some persons that all containers could or should be inspected prior to their loading in a foreign port or prior to their release from the U.S. port of arrival, it is not operationally or technically feasible, nor commercially practical, to inspect all, or even a majority, of maritime containers. Furthermore, the Subcommittee is not aware of any credible proposal that would allow all 8 million inbound U.S. maritime containers to be inspected in a commercially operable manner in the foreseeable future. The importance of ATS as the tool that determines which containers warrant further inquiry is thus of the highest importance.

²¹ The term container “inspection” includes both the physical de-vanning and inspection of container contents and inspection using non-intrusive inspection (NII) technology equipment.

We recognize the comment of *The 9/11 Commission Report* which, when addressing transportation security, stated until security enhancement technologies “such as scanning technologies designed to screen containers” can be deployed on a widespread basis, “the best protective measures may be to combine improved methods of identifying and tracking high-risk containers, operators, and facilities that require added scrutiny....”²²

ATS decides what cargo should not be loaded aboard the vessel at the foreign port, what cargo needs to be inspected at either the foreign port or the U.S. discharge port, and what cargo is considered low-risk and able to be transported expeditiously and without further review. Its function, effectiveness and credibility are a cornerstone of the U.S. government’s approach to container security. Enhancing ATS also fulfils the statutory directive of the MTSA, specifically, that “secure systems of international intermodal transportation ...shall include ... screening and evaluating cargo prior to loading in a foreign port for shipment to the United States either directly or via a foreign port” (46 U.S.C. 70116(b)(1)), and that the Department “shall develop and maintain an antiterrorism cargo identification, tracking, and screening system for containerized cargo shipped to and from the United States....” (Section 111 of the MTSA).

Another factor demonstrating the importance of enhancing ATS is the provision in the Coast Guard and Maritime Transportation Act of 2004, which provides that the DHS Inspector General is to analyze ATS, and if the IG determines that “the targeting system is insufficiently effective as a means of detecting potential acts of terrorism utilizing international intermodal containers”, then within 90 days after that report, the Secretary of the Department of Homeland Security shall submit to Congress a report identifying what actions will be taken to correct deficiencies.

For ATS to provide enhanced security screening, the system should acquire additional shipment data to be used in the pre-vessel loading security screening process. ATS uses information gathered from different sources; however, the data that must be provided by commercial parties for each shipment’s pre-vessel loading security screening is currently comprised of 15 cargo data elements from the carrier’s bill of lading filed in AMS by the carrier:

- a. Shipper’s name/address
- b. Consignee’s or owner’s name/address
- c. Notify address
- d. Bill of lading number
- e. Marks and numbers from b/l

²² *The 9/11 Commission Report*, page 392.

- f. Container number and characteristics
- g. Seal number
- h. Cargo description
- i. Hazmat code
- j. Gross weight or measurement
- k. First foreign port/place carrier takes possession
- l. Foreign port where cargo is laden aboard
- m. Foreign discharge/destination port for TE/IE cargo
- n. Piece count
- o. In-bond data if IT/TE/IE cargo

While bill of lading data and the existing 24 Hour Rule were an appropriate place to start, bill of lading data filed in AMS should be supplemented in order to provide better security risk assessment.²³

For private sector parties, the issue in enhancing ATS is what additional information do they need to provide Customs, when, in what system. Currently, there is no data required to be filed by the U.S. importer or foreign exporter that can be used at this stage of the security screening process, and there are shipment data elements of apparent relevance that bills of lading do not and cannot capture. While it is important that one not overwhelm the system with data that is of doubtful or minimal security screening value, the following data elements, which are not currently received by the government in time to be used in the security analysis, would seem relevant to the security analysis targeting system:

²³ See also, "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection", General Accounting Office Report and Testimony. March 31, 2004 (GAO-04-557T).

Shipment Data Need	Data Source, Provider, and System
1. Better cargo description (carrier bill of lading data in AMS is not always specific or precise)	Merchandise entry information/importer
2. Party that is selling the goods to the importer	Same (already identified by CBP in Trade Act regulations as desired information)
3. Party that is purchasing the goods	Same
4. Point of origin of the goods	Same
5. Country from which goods are exported	Same
6. Ultimate consignee	Same
7. Exporter representative	Same
8. Name of broker (would seem relevant for security check.)	Same
<p>9. Origin of container shipment – the name and address of the business where the container was stuffed.</p> <p>Today, this is often not available from a bill of lading. For example, it is not available on port bills of lading. It is not available with merchant or forwarder controlled haulage (prevalent in Europe). It is not available when carriers are switched to make the final move to the U.S. It can be hidden from ATS by changing the transportation contract.</p> <p>In the absence of a bill of lading starting at the door of the location where the container was stuffed, this data element is presently unavailable via AMS. Thus, for example, a shipment originating in Country A, may be transported on one inland bill of lading to a port in Country B, and a separate “port” bill of lading created showing the origin of the shipment as the load port. The bill of lading information filed in AMS will show that load port as the origin. It is the origin of that transportation segment, but not the origin of the shipment.</p> <p>It is not possible to get this information from the manifest filing system in the absence of a “door” bill of lading. The carrier does not have this information. This appears to be a significant shortcoming of the current system.</p>	<p>Admittedly, the answer is not simple.</p> <p>One option would be for the importer to file this information with Customs along with the other data elements identified above. However, there will be times when the importer may not know this information.</p> <p>One option would be for the carrier to file this information, but, unless this is a “through” bill of lading move, the carrier is unlikely to know this information.</p> <p>If DHS concurs that it is important to the enhancement of ATS to obtain this data element, a working subgroup could be established to consider the matter further.</p>
10. Identification of seal anomalies: such as broken or missing seals, or seal number not matching the seal number identified in the shipping documents.	This is what is being proposed by the industry in the MTSA Subcommittee Deliverable #1 recommendation.

MTSA Subcommittee Recommendations to COAC.

Data elements 1-8 identified in the chart above are within the shipper's knowledge and control, not the carrier's. Customs itself has stated: "Entry data is some of the most detailed and accurate information available for targeting...."²⁴ The problem is that this data is currently not filed in time to be utilized by ATS prior to vessel loading (often it is not filed until after the container reaches its U.S. inland destination), yet the law requires the cargo security screening and evaluation system to be conducted "prior to loading in a foreign port".²⁵ A more credible and robust targeting system used before vessel loading in the foreign ports would appear essential to any credible contingency response and planning capability.

Data Element 9 concerns the origin of the container shipment, including the identity of the party who stuffs the container. It involves relevant data for a security analysis, but the best means to obtain this information is not entirely clear. If DHS concurs, a Working Group could be established to consider this issue further.

The MTSA Subcommittee Recommendation on Deliverable #1 addresses data element 10.

RECOMMENDATIONS:

1. Customs should advance the time for importers to file data elements 1-8 to at least 24 hours before vessel loading, just like bill of lading data filing by carriers in AMS was advanced to before vessel loading under the "24 Hour Rule."

2. The early filing of shipment data elements 1-8 (or others as may be required) by U.S. importers or their agents should not be considered to be formal or final merchandise entry declarations until such time as such declarations are legally required, and should be used solely for cargo screening and targeting or other security purposes. Early data filings of this nature are for the purposes of counter-terrorism, and for that reason, should not be permitted to be used by CBP to monitor or enforce trade compliance, as that would undermine the intent of the early information filing. While data may change subsequent to this early filing, filers should nevertheless undertake to provide the best, most accurate data available.

3. The change involved with the early reporting of data elements 1-8 by importers or their agents is significant and may require some importers to substantially modify their commercial operations and systems, thus, the

²⁴ Testimony of Assistant Commissioner Jay Ahern before the House of Representative's Energy and Commerce Committee's Subcommittee on Oversight and Investigations, March 2004.

²⁵ 46 U.S.C section 70116(b)(1).

Department should implement and enforce the reporting requirements in phases to effectuate a smooth transition.

4. Due to disparities in importers' supply chains, it may be difficult for some importers to comply with the timing for reporting the data elements set forth in recommendation number 1. Therefore, specific guidance should be provided by Customs as to what would be the implications if data elements 1-8 are not provided to Customs 24 hours prior to vessel loading. In determining the implications for a failure to report that data, Customs should take into account whether the importer and other involved parties participate in C-TPAT and whether other existing security programs and measures apply to the involved shipment.

5. It is essential that CBP's existing data systems, and new systems that are used to support screening and targeting functions be provided adequate financial resources, and that all necessary programming be performed with adequate lead time to allow industry to adapt to any changes in technology or processes. Fortunately within CBP the development of the new system Automated Commercial Environment and International Trade Data System (ACE/ITDS) is well underway. ACE/ITDS provides the system through which the trade community will submit in the future commercial data to CBP and ITDS participating agencies. ACE was originally authorized by the Congress in the Customs Modernization Act of 1993. The need for better cargo security brought about by the events of 9/11 have increased the urgency for ACE/ITDS. The trade community has supported ACE/ITDS through the Trade Support Network created by CBP and has significantly invested in its development. The MTSA Subcommittee endorses ACE/ITDS and recommends its funding be increased significantly, as had been originally planned. Completion needs to be accelerated to meet the importance of the system to government and industry in a post- 9/11 environment.

6. DHS should consider whether to establish a Working Group to further analyze the feasibility and value of requiring the reporting of the Origin of the Container Shipment (data element #9), including the name and address of the business where the container was stuffed, prior to vessel loading.

In addition to the above recommendations, there are a number of questions concerning the proposed reporting of the additional data elements, including:

1. Are there additional data elements, not included above, that should be routinely acquired for ATS security screening? If there are other data elements that DHS has determined are also needed to enhance the ATS security screening analysis, they could be identified and addressed in a similar manner – enabling a discussion for the purpose of identifying who should file the data, when, to what government system.

2. Are the identified data elements above of sufficient value to ATS security screening that they should be obtained prior to vessel loading, or can some be eliminated?

The MTSA Subcommittee's preference would have been for DHS to identify to the Subcommittee those additional data elements the government had identified it needed to enhance the effectiveness of containerized cargo shipments' security screening. In the absence of such information from DHS and in recognition of DHS' request that the Subcommittee provide DHS with a recommendation in this regard, the Subcommittee requests that DHS confirm that each of the data elements identified above would be of value in enhancing the security screening of maritime containerized cargo. In addition, the Subcommittee requests that DHS confirm whether data element #7 (exporter representative) would be of value, and if so, to precisely identify what parties would be acceptable to be named in this category. The Subcommittee notes that the data element definitions will require further precision if the government determines to propose regulations to implement these recommendations. The Subcommittee notes further that, where possible, required security data elements should be satisfied by the use of commercially used data elements.

2. Proposed Objective #2: Effective security cooperation and coordination between governments through an effective CSI program.

We strongly support CSI and commend the governments of the United States and other trading nations that are establishing such agreements. Because these are government-to-government arrangements, the industry does not have a direct role in their implementation. If there is to be an international structure for trading nations to cooperate on container security review and inspection – which we believe is essential, it is difficult to see what alternative operating mechanism would exist if CSI is not developed into an effective, working cooperative mechanism. The World Customs Organization is working in this area in a supportive manner, but tangible results are slow and elusive, and operational implementation and coordination requires the CSI. The MTSA Subcommittee recommends:

1. Continue progress on making CSI ports operational. Today 20 of the 38 CSI ports are operational.
2. Add other significant ports to the CSI network.
3. CSI implementing governments must discuss, understand and agree upon respective expectations and necessary capabilities of

these agreements. In this regard, CSI is an important component of compliance with the MTSA requirement that “secure systems of transportation”, include “procedures for allowing the United States government to ensure and validate compliance” with programs designed “for screening and evaluating cargo prior to loading in a foreign port”. (46 U.S.C. 70116(b)(4)).

However, U.S. Customs must be able to demonstrate to the Department of Homeland Security, the Congress and the American public that foreign CSI Ports conduct more than a *de minimis* amount of examinations and inspections.

CBP inspects approximately 5.6% of the inbound maritime containerized cargo shipments or roughly 450,000 containers/yr. A percentage of those inspections are for security reasons; however, the vast majority of those security inspections are in the U.S. port of discharge rather than the port of loading. What is the explanation for this? What are the expectations of both the exporting country and of the United States going forward regarding inspections before loading at foreign ports? How much non-intrusive inspection equipment is needed for a CSI port?

4. In the event of a terrorist incident involving maritime commerce, what will CBP and the U.S. government expect of CSI ports regarding cargo security? Will CBP require significantly more container inspections at foreign ports before vessel loading? If so, has that been communicated to the foreign ports? Similarly, have foreign countries identified and communicated their expectations to the United States for its exports? CSI nations need to discuss and understand each other’s needs and expectations and plan how they may be addressed. For example, how much Non-Intrusive Inspection equipment, such as VACIS machines, is needed in a CSI port? Should there be specific standards with regard to inspection goals based on, for example, port volumes and risk assessments?
5. Are security screening criteria being used by CSI government authorities coordinated and consistent?
6. What are the ramifications of not being an operational CSI port? This is not entirely clear. CSI participation is not a condition of trading with the United States, even if the U.S. is responding to a container security incident. Similarly, it would not seem correct simply to say that in the event of a security crisis, only commerce originating in an operational CSI port would be admitted.

Operational CSI ports exporting to the U.S. currently account for roughly 40 of the United States' containerized imports. Surely, shutting down trade with all non-operational ports, including all of Latin America, Australia, New Zealand, and the Indian Subcontinent, and most of Africa and the Middle East is neither an attractive nor viable option. But what would the treatment of such commerce be in an emergency? What role should or could a multilateral CSI system play in this regard?

A reasonable approach to consider might be as follows: Customs can issue "Do Not Load" messages to carriers regarding cargo to be loaded in CSI and non-CSI ports equally. As the Automated Targeting System (ATS) matures, and in elevated security conditions, presumably more cargo would be given "Do Not Load" messages. CSI provides participating, operating ports a mechanism to not only exercise prevention and interdiction capabilities, but to address such cargo and any questions about it -- in other words, examination and inspection -- so that it can be loaded aboard a vessel for the U.S. after examination. Non-CSI ports do not have a pre-existing mechanism to address such issues, and cargo in these ports that is given a "Do Not Load" message would seem to have no certain way to be cleared for vessel loading.

7. Each CSI port should have a 24x7 problem resolution capability.

3. Objective #3: Develop transparent, measurable requirements defining a "secure" shipment entitled to "green lane"²⁶ treatment and for contingency planning – Define a "Safe and Secure" cargo shipment

It is important to carriers and shippers alike to know what criteria should actually serve to produce "green lane" treatment, especially as it would seem logical that such criteria would be used by the government to manage the continued flow of international containerized cargo in the event of a terrorist incident involving one or more container shipments. If such an event were to occur today, the industry would not know what cargo could be loaded in a foreign port with assurance that the vessel and cargo loaded would be able to be

26 The Subcommittee recognizes that the federal government, working with industry, needs to develop a clear definition of the "green lane" concept, including its specific attributes and benefits.

discharged and released expeditiously upon arrival in the U.S. It is important to the international economy and supply chains that these issues be addressed.

The industry knows that the ATS currently screens all cargo before vessel loading, but a tiny percentage of containers are given “Do Not Load” messages in foreign ports, and 94.4% of all import maritime containers are not inspected. 5.6% of imported maritime containers are inspected (meaning by physical inspection or NII inspection technology). If that would change in the event of a security emergency, the industry presently has no understanding of what it would be expected to do. Carriers, shippers and terminal operators would all benefit from having some better understanding of expectations so that contingency planning can be facilitated.

One way to approach this issue of defining what is a “secure shipment” would be to consider what transparent, predictable criteria should result in containerized cargo shipments having assured security. It would appear necessary in such an effort to include criteria for what needs to occur at container stuffing in order to be provided “green lane” treatment, as that process is both beyond U.S. regulatory jurisdiction, and industry currently lacks clearly understood and enforced criteria. The following example is provided only for the purpose of illustration, and assumes that enhanced ATS is implemented as discussed above.

Category A Containerized Cargo Shipments: These would be containers of cargo that the government and the shipper can be sure are secure and allowed to move both with “green lane” treatment under normal operating conditions, and could have reasonable assurance of vessel loading at the foreign port of loading and expeditious release at the U.S. port of discharge, even in the event of a security incident. Absent specific contrary intelligence, these containers could be assured that there would be no need for inspection or delay. The following criteria specifically address the container loading procedures and verification.

Possible requirements for this highest level of security consideration:

- A. Port facility and vessel must be ISPS Code compliant. The port must not have been determined by the Department of Homeland Security, pursuant to 46 U.S.C. 70108, to be not maintaining effective antiterrorism measures.
- B. Importer, broker, and carrier must be enrolled in C-TPAT (The Subcommittee recommends that each such C-TPAT party be validated, as well as enrolled, in C-TPAT. Recognizing that validation is an ongoing process, the Subcommittee wishes to emphasize the importance of an effective validation process that all parties can participate in time to meet this requirement.)

- C. The exporter/party stuffing the container must:
- i. be enrolled in C-TPAT, or
 - ii. be recognized by the foreign exporting nation as being a secure shipper pursuant to agreement with CBP, or
 - iii. have the importer file with CBP via the ABI system prior to vessel loading a confirmation that the cargo loading process was secure and witnessed either by a certified, third party inspector (from a list of inspectors acceptable to Customs) or from an employee or agent of the C-TPAT importer who is present at container stuffing, and
 - iv. affix, at the conclusion of the container stuffing process, a high security seal meeting ISO standards (PAS 17712).²⁷
- D. The container is subjected to radiation screening by foreign customs before vessel loading. (Question for CBP: The Subcommittee recognizes that the U.S. government has stated that it intends to perform radiation screening on 100% of all inbound containers. The Subcommittee defers to the judgment of the government how best to maximize the occurrence of such screenings before vessel loading.)
- E. The container has been subjected to seal verification pursuant to Deliverable #1 and no unexplained anomaly exists.

[Note: While building on existing ISPS Code and C-TPAT initiatives, this would impose requirements relating to the container stuffing process that do not exist today. It would address DHS' question in Deliverable #2 regarding "private equivalents (such as third party inspectors initiated by private sector supply chain entities)", but provides that such inspectors are only one option for the shipper. Unless the container stuffing process is addressed, it is unclear how one can be confident that the containerized cargo is secure, or that any of the subsequent measures that carriers may be expected to implement while the container is in their possession will have value.]

Category B Containerized Cargo Shipments: These cargo shipments could generally be accorded, but not guaranteed, "green lane treatment". These containers are likely, but not guaranteed, after ATS screening by Customs, to be loaded aboard the vessel in a foreign port in the event of a container security incident. These containers may be subject to VACIS or physical inspection at the

²⁷ Specifying the ISO PAS 17712 as the standard, as proposed in the MTSA Subcommittee's Recommendation for Deliverable #1, would fulfill the MTSA's provision stating that the Department should develop "performance standards to enhance the physical security of shipping containers, including standards for seals and locks". (46 U.S.C. 70116(b)(3)).

loading port or on arrival at the U.S. discharge port, but the expectation would be that they generally would not need to be. Requirements:

Same as Category A Shipment, except Item C (i-iii) is not required.

[Note: This is basically C-TPAT, with validation and a mandatory high security seal affixed at stuffing and radiation screening, and seal verification as proposed in Deliverable #1. It may not provide an ideal level of security, but we have been unable to identify a better middle ground category. If we do not strengthen C-TPAT, what would take its place?]

Category C Containerized Cargo Shipments: There are unlikely to be sufficient volumes of Category A and B containers to fill a vessel. Accordingly, the 24 Hour Rule and an enhanced ATS pre-load security screening system are essential to review a wide range of other scenarios (Category C). Other than an enhanced ATS system that is entrusted to determine what gets loaded and what gets inspected, we do not have recommendations for how this cargo should be treated, other than the following suggestions:

- (a) ATS should be strengthened as recommended in Part II above. It should issue “do not load”, “inspect at load port”, or “inspect at discharge port” as appropriate.
- (b) If a Category C container has been inspected at the load port by an entity acceptable to Customs and no security issue is identified, it should be allowed to be loaded and should not be subject to inspection again upon arrival in the U.S.

Elevated Security Conditions

In the event of a substantially elevated security condition (Condition Red) involving international containerized commerce (hopefully coordinated with the U.S. Coast Guard), containers in Category A, or Category B or C(b) need to be assured that they can continue to be transported. Any container not in one of these categories should be issued a “Do Not Load” message if there is a reasonable basis to conclude that it would cause the vessel’ entry or its unloading in the U.S. to be put at risk. This would at least give the government, the trade, the vessel, the terminal operator and the Category A, B and C(b) cargo the assurance that a level of operations and trade, which has undertaken steps to satisfy the government that it is “secure”, can be counted on and that entry of such cargo into the U.S. would be facilitated. All other containers would “take their chance”.

The above is a draft, preliminary starting point for this discussion. It certainly would need to be modified and improved, but it attempts to begin identifying clear, predictable criteria that help to produce assured loading, discharge and release of cargo shipments.

4. Objective #4: Effective contingency planning for how the U.S. government would keep its foreign commerce flowing in the event of a terrorist attack on or using a container.

This is a most important issue and presents the means to address many of the underlying strategy questions, including as noted above, the issue of respective responsibilities.

The issue of contingency planning is one that everyone in the supply chain is currently questioning. As industries look to develop their own contingency plans in the event of a terrorist attack, we need to know what to expect from the Government if an event were to happen involving a maritime cargo container.

It is the hope of the trade community that the U.S. government has plans that would keep legitimate global commerce moving if an incident were to occur. There have been several incidents that the U.S. government can learn from as to what happens when the entire transportation system is forced to shut down. From the grounding of the airlines on September 11th, to the West Coast port lockout in 2002 to the most recent incident in NY with the container ship CSAV Rio Puelo, there needs to be a coordinated effort to ensure that an incident does not shut down commerce.

Everyone involved in the supply chain from the U.S. Government to Foreign Governments to members of the trade community have certain responsibilities that need to be accounted for if an incident occurs.

Federal, State and Local Government Responsibilities

First and foremost, the biggest question on the trade community's mind is who will be in charge and make the decisions if an incident occurs? Will it be the Captain of the port where the incident occurs? If not, will decisions come from DHS headquarters? What is the role of state and local agencies if an incident occurs, and what is the authority of such agencies vis-à-vis the federal government in making these decisions? What about surrounding ports? If something happens in the Port of Los Angeles, what would be required of ports on the East coast? What criteria will be used to determine what U.S. trade will be allowed to move in the event of a security incident?

If an incident were to occur in the Port of LA, that port as well as the Port of Long Beach might have to be shut down during the incident investigation and response. What would happen to other ports on the West Coast? Would Seattle/Tacoma remain open? Would incoming cargo be able to be diverted to other ports? While the individual ports have worked on contingency plans for their facilities, have there been discussions among ports geographically located

near each other as to how the ports would work together? Will all maritime vessels be required to stop where they are or will vessels at non-incident ports be allowed to continue to move?

It is not clear to the trade community at this point in time as to who will be making the decisions. This needs to be shared with the trade community so that they can plan appropriately.

We need to know what the role of each federal agency involved in the supply chain (DHS, Coast Guard, CBP, TSA, FDA, etc.) , as well as state and local agencies, will be in the event of an incident. There needs to be a clear line of communication among the agencies and to the trade community so that we know who is in charge and making the ultimate decisions. We do not want to find ourselves in a position where the Coast Guard makes one decision while CBP would make another. The trade community needs to know exactly which agency will make which decisions.

Foreign Government Responsibilities

In addition to the role of the U.S. government, we also need to know what the U.S. will expect and require of foreign governments if an incident were to occur. Will cargo from CSI ports be handled differently than those from non-CSI ports? Will cargo continue to be loaded at foreign ports if an incident occurs? If not, where will the cargo go? Many foreign ports do not have room to store cargo containers for long period of times.

U.S. Industry Responsibilities

While there are many questions that we have as to the government's responsibilities, we also need to know what will be expected of U.S. industries?

What will be expected of carriers and marine terminals? What about shippers and importers? What about other modes of transportation to and from the port facility? What about transportation through non-maritime ports of entry? Will the northern and southern border ports of entry be closed down? Who should the trade contact if an incident occurs? The Captain of the port? Local CBP officials? Coast Guard? Will there be direct communications with the trade on what to do?

U.S. companies already have contingency plans in place for events not related to terrorism (natural disasters, etc.), but many of these plans can be adapted to handle an issue of terrorism. We just need to know what to expect from the federal government as to whether or not all cargo will stop moving or if it only pertains to the impacted port.

There are many more questions that need to be asked, but we need to start with the basic dialogue first and identify the main concerns of the trade and how to work through the challenges to ensure that legitimate global commerce continues to flow if an incident involving a maritime cargo container were to occur.

5. Objective #5: Addressing non-maritime transportation within the intermodal system of transportation

The “intermodal” transportation system is not a seamless, single stream of transportation, but rather various transportation sectors operating in conjunction through a variety of exchanges to move cargo from origin to destination.

The MTSA Subcommittee has been requested by DHS to focus on intermodal transportation that has an international maritime segment, and our recommendations reflect that focus. The Subcommittee also recognizes that the security of land transportation of intermodal containers, both in foreign countries and in the United States, is relevant to a secure transportation system; however, recommending new security regimes for land transportation companies around the world and domestically was, in the opinion of the Subcommittee, beyond our scope or ability to address in this report.

Foreign Modal Interchange Operations

As noted in the MTSA Subcommittee Deliverable #1 document, “Short Term Minimum In-Transit Container Security Enhancement”, the Subcommittee recognized the limitations of U.S. government agencies to “legally require truck and rail operators in foreign jurisdictions to perform a particular action”. Recognizing this fact in deliverable #1, the MTSA subcommittee recommended to DHS that, for the purposes of securing a container, the department should “require by regulation that the ocean carrier or its agent verify the shipper-applied container seal before loading a container into a vessel bound for the U.S.”

In addition to the application of a seal verification regime, the Subcommittee has proposed expanded and closer CSI relationships with the governments of our trading partners (including enhanced container inspection capabilities at foreign ports), enhancement of containerized cargo targeting system capabilities, a proposed vision for future “smart shipment” technology developments, and more specific definition of “green lane” criteria, including a proposal for securing the shipper/point of stuffing. The Subcommittee was unable to fashion a practical recommendation to address the numerous foreign trucking, rail and barge movements of containers moving in other nations’ jurisdiction. At some point in the future, C-TPAT might evolve to include this portion of C-TPAT shippers’ supply chains, but the Subcommittee did not believe it was currently practical to recommend that C-TAPAT consider enrolling truck, rail or barge transportation companies offering services in foreign countries.

Although the Subcommittee recognizes these limits of jurisdiction, we encourage the U.S. government to work with our international trade partners to consider ways to augment the security of the international supply chain.

U.S. Domestic Modal Interchange Operations

DHS' request that the MTSA Subcommittee consider the movement of containers through international supply chains logically includes the movement of international containers as they are transported domestically in the United States.

Containers of cargo arriving at U.S. maritime ports on a ship have to move by rail, and/or truck for delivery to their final destination or for further transportation. The important government security clearance is, not when the goods make formal entry into the U.S., as that could be many days after the cargo leaves the port. The most important security clearance is when CBP releases the cargo from the port of arrival for further transport.²⁸ The Automated Targeting System, and all the other programs and recommendations discussed in the Subcommittee's recommendation, will have been applied by the time the container is released from the port of discharge, including the possibility of container inspection by CBP at the arriving port. The necessary underlying assumption is that shipments released by CBP into the U.S. for further handling via the domestic transportation system are deemed to present no unacceptable risk. Once these shipments are released and enter the domestic transportation stream, there is no discernible reason for rail or truck operators to treat them differently than any other domestic shipments.

The MTSA Subcommittee believes that, for the purposes of expanding "security programs" to other segments of the domestic transportation industry, such an objective is beyond the scope of this subcommittee and the COAC. Such a major undertaking needs to be closely coordinated with other federal advisory committees on transportation, involve industry participants from the various Information Sharing Analysis Centers (ISAC) and upcoming Security Coordination Councils, the modal agencies within the DOT, and other groups of interest in protecting our nation's transportation infrastructure.

Transportation Worker Identification Credential (TWIC)

DHS is currently working on the Transportation Worker Identification Credential (TWIC) system to improve the ability of government agencies and carriers to screen the background of transportation personnel.

The Subcommittee recommends that the Department give the implementation of this program more urgent priority to ensure that

²⁸ The Subcommittee recognizes that many container shipments move "in-bond" with Customs, and that DHS has identified "in-bond" transportation as a component of some supply chains. The issue of "in-bond" movements was not analyzed or discussed in any substantial way by the Subcommittee.

transportation personnel within the United States who enter/exit secure transportation facilities have been vetted through a background check process. While the TWIC program will affect more than intermodal transportation with a maritime nexus, the Subcommittee believes that this national, uniform program would provide relief from the myriad of uncoordinated, security programs requiring background checks when operating throughout the intermodal environment. It is critical that the program be developed in close consultation with industry (the trade) to ensure that the system achieves its security goal without undue burden to any stakeholders.

Container Security “Smart Shipment” Technology

As part of its deliberations on Deliverable #2, the MTSA Advisory Subcommittee was requested by DHS to consider technology and its application to the issue of the “performance standards for a ‘smart container’ concept”, as well as specific questions regarding deployment, cost-benefit considerations, and whether such standards should serve as a security baseline or should be considered as part of a voluntary or incentive based approach (i.e., as part of C-TPAT or otherwise).

DISCUSSION

A “smart box” implementation would require new standards and procedures and would require clearly addressing the following issues, which at this time remain unresolved:

a) Clear and agreed definition of the requirements of a “smart” box.

Our understanding of CBP’s current view is that a “smart” box is one with an RFID electronic device that, when read, informs if the container doors have been opened. A more expansive definition is a container with an electronic device that, when read, informs if there has been intrusion into the container via any of the container’s six sides. An even more expansive definition is a container with an electronic device that not only detects intrusion, but has sensors that can range and vary in description from temperature and humidity, to radiation detection, to explosives detection, to ammonia and carbon dioxide detection, and which may also include GPS location readings, in addition to detailed supply chain and cargo information. Definitional clarity is needed.

An important question is one of establishing agreed goals: Is the “smart” box intended to address only the issue of in-transit intrusion of the container, assuming the container stuffing was secure, or does it include supply chain information, or does it also include sensor technology to identify whether

something bad was included in the container stuffing process? Does it include GPS capabilities? Does it include the provision of information about the cargo? These issues obviously affect the technology requirement. Furthermore, if factors other than intrusion are to be sensed, one must analyze whether fixed land based technologies and applications aren't a more efficient and reliable way to sense the factor (e.g., radiation sensors are currently being deployed at U.S. and some foreign ports to inspect 100% of all containers), rather than relying on devices on a globally dispersed 17 plus million unit container fleet that are potentially subject to malfunction.

b) Who "reads" the electronic device and where is it read?

Are Customs officials the parties that should read the devices in order to ensure security? Will the government trust private parties to read the security devices and report any anomalies? Where must the readings take place? To whom do the anomalies get reported? Who resolves them?

c) What kind of infrastructure is needed to read the devices?

If RFID technology were used, fixed readers at numerous locations around the world would be needed. Some RFID bandwidths are not available for this use in major trading nations. Carriers have identified major concerns about RFID as the infrastructure foundation for containers.

If the reading infrastructure is satellite based, many of the reading infrastructure and data ownership and access issues may be simplified.

If the reading infrastructure collects substantial data about the shipment, as well as the security data elements, who will have access to the data which the device generates?

d) Does "smart" container technology involve and include supply chain management information to meet the needs/demands of shippers?

E-seals should only address security information requirements and should not include supply chain information and complications. The ISO has embraced this approach for its current e-seal standard setting exercise. However, in the context of a "smart" box's use of an electronic container security device (CSD) that is more than a seal, there is an interest by some shippers – and seemingly all technology developers -- to have a device using wireless or satellite technology that can contain supply chain information details, include the security function of container intrusion detection, and have GPS location reporting capability. Such capabilities in CSDs could change how one approaches Questions 2 and 3 above (as the shipper is unlikely to want terminals and carriers having access to such data and will want the data communicated directly to the shipper).

One cannot dismiss these questions by stating that the government will set the overall requirement (e.g., a container security device that detects intrusion shall be installed on every container arriving in the U.S.), but will take no position on how it is to be read, by whom, pursuant to what protocols. There has to be agreement on how the requirement, once established, would be implemented – especially if disparate technologies can be used to meet the requirement. For example, Box A has a RFID device that operates at a bandwidth of 433 MHZ and uses geographically fixed readers overseas; Box B has an AllSet device that operates at 2.4 GHZ and utilizes a different fixed reader system; Box C uses NaviTag, a cargo-centric satellite system device, which provides readings directly to the shipper; and, Box D uses a different cargo-centric wireless or satellite device.

Furthermore, the 1972 Customs Convention on Containers provides that signatory nations, including the United States, must admit a container that is found by another signatory to be compliant with the convention. Thus, the implementing mechanism for any CSD that is to be attached to a container must be carefully analyzed, because it cannot be required as a matter of entry under the terms of the 1972 Convention and other related international instruments. Clearly, other means exist to implement the objective when it is defined (e.g., a shipment without a CSD will be subject to VACIS examination), but the issue illustrates that there is a need to recognize that this is international commerce that needs internationally understood and accepted rules. A requirement by the U.S. to attach a device that is not acceptable in another country (e.g. using an RFID bandwidth that is not publicly available or is otherwise restricted for such use in that country) could result in that country refusing admission to the container carrying a U.S. export shipment to that country. The issue warrants consultation and consideration.

“Smart” box implementation of container security devices requires, at a minimum, that agreement be reached on the following:

Does the government perform the reading of the CSD, or is this a function that the government is comfortable delegating to private sector parties?

If it is a private sector function, what requirements apply? For example, if a satellite system were used, would container intrusion detection reports be automatically fed to both the private party and CBP? Would the government accept not being on direct distribution of such information but rely on the private party to report any problems?

Would the carrier be involved in the device’s reports? What role, if any, does the carrier have if the technology is a “cargo-centric” device?

What protocols would govern actions that may be warranted by information obtained from the electronic device. For example, assume

that the device informs that the container doors have been opened at some point in transit. Who determines whether there is an acceptable explanation of the event or not? There has to be some judgment applied, but whose? Is it the shipper's? Is it CBP's? Is every box that has its doors opened in transit automatically subject to a VACIS exam?

Is the "smart" box concept implemented through a voluntary program, such as C-TPAT, or a mandatory, universally applied set of requirements? Is this a "smart container" concept or a "smart shipment" concept?

We are not opposed to the application of new technologies that can effectively enhance security, but we believe that the issues above must be addressed in partnership with the industry before a program is implemented. Furthermore, application of such technologies to international commerce requires any approach to be internationally acceptable.

RECOMMENDATION

The following is a recommended outline of how the "smart" container issue be addressed:

Step 1: As advocated in the MTSA Advisory Committee proposal on seal verification, the government should require that all containerized cargo imported into the U.S. be subject to the proposed seal verification process. "Smart" box technologies are not ready to be deployed in broad commercial practice in the near term. The debate on new technologies should not delay the implementation of measures to enhance the present state of in-transit container security.

Step 2: Define the "smart box" CSD vision:

1. A container cannot be made "smart" by simply adding a device to it. "Smart" involves an information system and its management. The "smart" shipment system must address the characteristics of a particular shipment. The terminology should refer to "smart shipments", not "smart containers".

2. Shipper, importer and technology interest in "smart" shipments all involve shipment information that is detailed and proprietary, and outside the knowledge and control of the carrier. It is this information that provides supply chain benefits to the shipper. Shippers will have legitimate concerns with such data being available or accessible in carrier or terminal operators information systems. These needs should be recognized and accommodated in the technology.

3. It is not practicable to outfit 17 plus million containers with such “smart” systems.

4. The shippers’ interested in the “smart” shipment are either shippers of high value or very time sensitive goods. The benefits relate to loaded cargo details for inventory verification, ability to search for commodities and their location, greater supply chain visibility, recorded access to the shipment, as well as improved container integrity monitoring. To achieve this, the “smart” system must involve parties and activities involved in stuffing and sealing the container. Those parties and procedures must be trusted for the device to have security enhancement credibility. Not every shipper will want to incur the cost and implement the procedures necessary for a “smart” shipment. Furthermore, different shippers will have different “smart” box needs (e.g., some may want temperature/humidity sensors, some would not; e.g., status notification needs would vary according to the individual supply chain’s needs and characteristics.)

5. We believe the government’s interest in the “smart” shipment should be to test and deploy such systems on a significant scale, and to use the “smart” shipment to provide further definition and meaning to C-TPAT’s “green lane” treatment. “Smart” shipments should get “green lane” treatment.

To accommodate all these needs, we believe the following could be a “smart” shipment standard:

A “smart” shipment involves a cargo-centric device²⁹ applied to a particular shipment by a C-TPAT shipper at its discretion, that does not require a network of geographically fixed readers at numerous locations around the world, but instead is read globally by satellite or wireless technology. The information system shall include the shipper’s very specific cargo details (it can be linked to RFID scanning of cargo loaded into the container), actual geographic location of the shipment (not the last time it passed a reader), detection of entry into the container via any of the container’s six sides, time and location recording of any entry into the container, and such sensors as the shipper may require. The frequency with which the device reports should be programmable by the shipper to be more frequent than a certain minimum, so that the device can report its status more frequently when in particular geographic areas.

²⁹ “Cargo-centric” means a device applied to a particular containerized cargo shipment at stuffing, which is removed at the shipment’s final destination and is re-used on a subsequent shipment loaded into a different container.

The information service centers that receive the data transmissions from “smart” shipments will provide the data to the shipper, not the carrier. Because of proprietary cargo and shipment information in such a device, shippers’ will have a need to restrict access to the availability of such data. They will not want numerous carrier and marine terminal data systems containing this data.

The government must determine what information events that are produced by the device, if any, that it wants to be notified of as a matter of course, and in what situations it is acceptable for the shipper or its agents to investigate and address any information events that arise (e.g., container door opened in China, and it is determined it was Chinese Customs).

The information service centers must meet standards acceptable to the government. (Perhaps a new C-TPAT category)

Because the reading of the devices is done remotely and not by the party with custody of the container, the carrier will not know, nor need to know, which shipments are “smart”. Accordingly, carriers would be required to perform seal verification on all containers before vessel loading as advocated in MTSA Advisory Committee proposal.

The shipper must inform Customs which shipments are equipped with “smart” technology, as part of the ATS Enhancement Recommendations made in the Council’s August 5 submission to the MTSA Subcommittee with respect to Deliverable #2, so that any favored “green lane” treatment resulting from the device could be provided to such shipments.

The devices are not permanent parts of the container, but are recycled. Who supplies the device and how to most efficiently recycle the devices would be left to the commercial parties to negotiate.