



WORLD SHIPPING COUNCIL
PARTNERS IN AMERICA'S TRADE

Comments in Response to Customs and Border Protection's Request for Information Regarding Smart and Secure Containers

February 17, 2004

I. Introduction

The World Shipping Council hereby submits the following comments in response to Customs and Border Protection's (CBP's) Request For Information for Smart and Secure Containers (RFI), published December 16, 2003. The Council fully supports the agency's efforts to enhance containerized cargo security and to examine how technology may be applied to meet that objective.

The agency describes the RFI as "for investigative purposes only" and specifically directs respondents to consider the "practicality of implementation", "operational impact", "estimated costs", and potential pilot test concepts.

We commend the agency for reaching out to affected parties in this manner and soliciting their input in the formative stages of this endeavor. The issues involved are significant, and a well-grounded investigation and analysis of the issues with the involved commercial parties is an essential foundation to a successful effort. Gathering more detailed information from the users and stakeholders of the international transportation system is essential for progress to be made on these issues, and we commend CBP for its inquiry. The invitation for industry input in this process is a productive and welcome initiative by the government.

It is in the interest of all involved persons to work with CBP and the Border and Transportation Security Directorate to establish clarity on what the security objectives are that requests for proposals for secure containers should meet, and, importantly, how those requirements and proposals can fit into the operating environment of international trade. The objective must be to build a more secure operating system that will work more efficiently. Concepts and proposals that do not reflect a commonly understood and shared set of objectives are not likely to produce progress. Proposals that do not attempt to address how the proposals would actually be applied to the operating conditions of international commerce are deficient.

The Council is committed to supporting a quality and effective analysis of these issues and of the best ways to enhance security, and strongly supports a coordinated analysis of these issues within the Department of Homeland Security. We also note that the in-transit security of containers is only one part of the issue. Secure *shipments* are really the objective more than secure containers, and this also requires secure cargo loading and sealing, accurate and timely documentation of the necessary shipment data from the party with direct knowledge, as well as enhanced screening and inspection capabilities.

II. WSC Response to the Request for Information

The Council's comments are limited to a five-page submission as specified in the RFI, but our Members are willing to meet and discuss these issues in greater detail with Department officials at any time.

A. Comments of General Applicability

As the agency further develops this initiative, we recommend that several issues of general applicability be clearly addressed.

1. *Is the objective to develop and deploy technology that can be used for security screening before vessel loading at foreign ports, and thus integrated into the 24 Hour Rule and CSI initiative, or is the objective of the technology to be used for security screening “upon the port of entry”, as stated in the RFI? The answer to this question will obviously have a substantial impact upon the scope of application and the number of entities in the global supply chain who would be involved.*

2. *There should be a clear explanation of the security objective that the technology is intended to attain and how it is superior to existing ways of attaining the objective.*

3. *The government needs to distinguish and separate the analysis and assessment of technology that may enhance container security from technology that may be a tool for enhancing supply chain information management. The issues, the challenges, and the requirements involved in addressing the two are not the same. The purposes and use are not the same. The technology, operational and information implications are different. A failure to clearly distinguish between security objectives and commercial applications will create confusion and ambiguity, will impede progress on these issues and, in fact, may create security vulnerabilities.*

4. *In order to structure an effective and meaningful analysis of proposals, CBP should insist that all technology proposals specifically and clearly address and identify how they and the information they generate are to be collected and used, including:*

- *What information is generated, who is authorized to generate it, and is that information necessary for security purposes?*
- *Who collects the information?*
- *What supporting infrastructure the technology requires and who operates it?*
- *Who has access to the information?*
- *What is done with the information?*
- *What actions are to be taken with respect to the information?*
- *What the costs of the technology and its use are, and who incurs them?*
- *How the technology affects the operations of shippers, carriers and the relevant government agencies?*

5. *Any technology selected must have a non-proprietary, open architecture allowing competitive sourcing of the product and its supporting infrastructure.*

6. *Proposals should understand and must realistically address the operational realities of the use of 16 million containers deployed in global commerce.*

For example, hundreds of thousands of containers are opened each year during transit for legitimate reasons, often by foreign customs officials. The design, use and application of security devices affixed to containers must address this reality.

For example, containers are “interchanged” between carriers frequently, and leased containers (which comprise roughly half the global container fleet) are hired on and off frequently.

For example, containers are not employed in dedicated or closed service loops, but are deployed throughout the world. A container may be used in the U.S. trade multiple times during its service life, once, or not at all. Technologies attached to a container for more than one shipment must consider this.

B. General Comments Regarding Cost

CBP has identified the cost of possible technologies to be a very relevant consideration, which is obvious and unarguable. The Council’s Security Advisory Committee in its consideration of these issues has identified several characteristics of various proposals that directly affect cost, and thus potential

desirability, of possible products. We recommend that the Department take them into consideration as it reviews this issue.

- When non-security features are added to devices, the cost of the device, the cost of the supporting infrastructure, and the cost of its use increase.
- Cost analysis must include not only the cost of a device, but its administration and use (including maintenance and repair), the number and cost of false positives, the infrastructure needed to properly utilize the device, and the protocols resulting from the use of whatever information is produced by the device.
- Unless the device is permanently affixed to the container, it should be designed for a single usage, and not reuse. Recycling devices from one shipment to another not only raises significant logistics and security issues, but also the cost and complexities of such recycling is likely to be unacceptable.
- The cost of deploying whatever technology is determined most appropriate to the international trade network will be substantial. Accordingly, there needs to be confidence that the government will not want to switch technologies soon after establishing what is desired.
- The supporting infrastructure for some technologies may impose significant costs on operations in other nations, and thus international cooperation on these issues, through the Container Security Initiative and other international governmental efforts, will be important.

C. General Comments Regarding Operational Impact

We strongly commend CBP for including in the RFI analysis and consideration of how a technology will fit into and work in the operating environment of international commerce. The Council's Security Advisory Committee has identified several characteristics that directly affect operations, and thus potential desirability, of possible products. It is essential that new technology enhance, not retard, operations.

- As noted above, hundreds of thousands of loaded containers are opened at some point each year before final delivery, often by foreign customs officials. A technology proponent must be able to adequately address that reality.
- The technology must be acceptable and available for use in the countries where shipments originate. For example, some RFID frequencies and bandwidths are not commercially available in some major trading nations.
- The technology must be functional in the operating environment in which it is deployed. For example, technology platforms that require line of sight to operate may have significant shortcomings in the operating environment.
- Technology that produces false positives will not be credible and will cause unacceptable operational disruptions.
- Operational assessments and implications must include not only the technology and the device, but the collection and use of whatever data is generated by the technology, including who collects the data, what is done with the data, who has access to the data, who can change the data, and what data the government wants from whom, when, and in what form.

D. Electronic Seal Recommendation of World Shipping Council's White Paper and the Council's Recommendation of a Test of Such Devices

In September 2003, the Council submitted a White Paper to CBP, the Transportation Security Administration and the Department of Homeland Security, entitled "In-Transit Container Security Enhancement".¹ The White Paper proposes an "off the shelf" concept for improving integrity and security of containers as requested in the RFI. The Council continues to recommend that White Paper for the government's consideration.²

¹ The White Paper can be accessed at the Council's website at www.worldshipping.org.

² The Council's White Paper did not address the issue of applying seals in a more secure manner than the traditional door handle application. We support CBP's effort to address that security issue through various alternative

The majority of the products and proposals for “improving integrity and security of containers”³ and enhanced “detecting intrusion en route” involve some application of Radio Frequency Identification (RFID) technology. The Council’s White Paper makes recommendations for regulatory changes that would address these security objectives without the use of new technology. But the White Paper also proposed specific characteristics for the optional use of electronic seals in order to address security enhancement objectives, namely that they: 1) have a unique seal number that can be both electronically and visually read, 2) record the date and time when the seal was activated or sealed, 3) record the date and time when the seal was opened or breached, 4) have “read” but not “write” capabilities, and 5) meet the high security manual seal standards in ISO PAS 17712.

We continue to believe that these are the appropriate security characteristics of an e-seal, and the Council and its member lines propose that, in collaboration with CBP, BTS and the appropriate officials of selected exporting nations, such seals be fully tested. We are confident that such devices could be made available promptly for this purpose. We would suggest that such a test be jointly developed with a small number of selected shippers, CBP and BTS, carriers and relevant port facilities to outfit all U.S. destination container shipments of such a shipper for a defined period of time with such electronic devices. We would suggest that the test involve an Atlantic and a Pacific trade component. We suggest that such a test be designed to address how such readings would be done in significant numbers in a normal operating environment. The Council is willing to help coordinate the planning of such a test.

The Council’s Security Advisory Committee continues to believe that the development and analysis of these kinds of electronic devices defined above is a sound security approach for the following reasons. First, e-seals, like manual seals, will be frequently broken to allow customs officials and other legitimate persons access to the container. E-seals, like manual seals, should not be reusable. The Council’s Security Advisory Committee believes that seals that allow persons with electronic devices to open and reseal the container seals appear to present an unacceptable security risk and to require an unenforceable security process around the world to control and monitor who has access to such devices or capabilities. Having a “write” capability in the seal also means that people can change the data in the seal, which also is a security concern. Including a write capability also requires additional power capabilities in the device and increases the cost of the device with no security enhancement. An effective container seal is a device that should be destroyed if it is opened.

We also understand, however, that RFID technology may be desired by some shippers for supply chain management purposes, and that such developments should be accommodated. However, separating those objectives from security objectives is important to obtain clear analysis and to accelerate progress in both areas.

Accordingly, the Council’s Security Advisory Committee recommends that the RFID tag and seal technology for international shipping containers be encouraged and addressed by separating the RFID devices as follows:

1) A passive⁴, read-only *RFID container tag* affixed by the container owner on the container and which remains permanently affixed for the lifetime of the container (except in situations where the container changes ownership). The tag should only contain “license plate” information such as container number, owner code and other information elements that today are included in the approval plaque on containers that meet existing IMO and ISO specifications (e.g. length, height, width, container type, mass).

applications. In that regard, the Council would again note its repeated request for CBP to publish the specifications for the so-called “Pardo hole”. We also note for this paper that the alternative e-seal locations must accommodate electronic seals.

³ We note that the RFI, these comments, and most technology proposals for enhanced container security do not address tank containers, flat racks, open top containers, palletized or break bulk cargo. Enhanced cargo risk assessment capability and enhanced cargo inspection technology do address those kinds of cargo as well as cargo in standard containers.

⁴ “Passive” means that the tag does not have a power source of its own. An “active” tag or e-seal has its own power source and thus is more expensive than a passive tag or seal. “Semi-passive” means that the tag or seal has a limited power source of its own, sufficient to record a basic set of data like the date and time a seal is activated or opened.

2) A semi-passive, read-only, non-reusable *e-seal* affixed to the container by the shipper for a particular shipment immediately upon stuffing of the container. The e-seal should possess the security characteristics identified above.

3) An active, read/write non-reusable *RFID cargo shipment tag* for that particular shipment affixed by the shipper on the container upon stuffing. Such tags should not be part of a seal, because seals when opened or broken will not and should not be reused, and thus supply chain data could be lost if it is tied to a security seal. Such tags would serve the shipper's/importer's supply chain management requirements. Accordingly, the standards for these tags should be left to the shipper community to formulate, including the identification of data elements to be included in the tag. Such a tag and its features, and all its many complexities and infrastructure implications, are not required for security enhancement, and thus can remain distinct from the effort to identify technology solutions that may enhance the integrity and security of containers. Whether such devices and their contents should be read by the same reader that reads e-seals is an issue requiring further significant analysis, including what authorized parties would have access to what data bases.

E. Sensors

The Council continues to consider how sensors might be applied to enhance container security, and while we have not reached any firm conclusions at this time, we would offer the following comments.

It is our assumption that seals will continue to be used on containers regardless of what kind of sensor may be developed, and that they will not be replaced by sensors.⁵ It is questionable to what extent and under what circumstances a sensor that only detects if a door has been opened would provide more useful information than a seal. A sensor that reliably detects if container intrusion has occurred by any means may be more valuable as discussed in the Council's white paper. Clarity on what must be sensed is obviously important, and testing of such devices will require further effort and evaluation.

The Council's Security Advisory Committee, however, would like to highlight the importance of ensuring that, if electronic seals are going to be encouraged, then the sensors should be capable of reporting their results at the same time through the same technology and system as the e-seals. Whether this is better done through a reader that can simultaneously read a sensor and an e-seal or through the sensor relaying its information through an e-seal (or vice versa), we have yet to form an opinion. But as CBP considers how to best to move forward with analysis and tests in this area, we urge the agency to require those who propose testing sensors to address this question of how the device would be read in a manner compatible with seal reading.

F. Inspection Technologies

CBP has been actively expanding its deployment and use of gamma ray and radiation detection container inspection technologies, as it has been steadily increasing its inspection of containers that it determines warrant more detailed examination. The Council agrees that this is an essential component of CBP's security strategy. As CBP continues to expand the number of containers that it inspects, we believe that the agency's technology inquiries should also include assessments of technology that may allow faster and more effective container inspections. This is necessary because, no matter how "smart" or secure a container might be while it is in transit, the greater security threat remains that something bad may be loaded into the container in the first place and then properly secured with a seal, etc. Accordingly, while we fully support the enhancement of security for containers in transit, we wish to restate our support for enhancing the government's cargo risk assessment capabilities and its container inspection capabilities.

⁵ We note that international agreements, such as the 1972 Customs Convention on Containers, and the 1975 Convention on the International Transport of Goods (TIR Convention), all signed by the U.S., require that when customs seals (or seals affixed by private entities in accordance with prevailing Customs requirements) are used, they are to be affixed to the exterior of the container.