



WORLD SHIPPING COUNCIL
PARTNERS IN AMERICA'S TRADE

Comments of the
World Shipping Council

Submitted to the
Department of Transportation
Transportation Security Administration

Regarding
Operation Safe Commerce
Docket Number TSA-2002-13827

December 5, 2002

The World Shipping Council strongly supports the federal government's efforts to enhance security for the movement of cargo through the international supply chains that serve American consumers and businesses. The Council and its Member liner shipping companies have supported the Customs Service's Trade Partnership Against Terrorism program (C-TPAT), and every Council member has applied to participate in that program. The Council and its Member lines have supported the government's Container Security Initiative and the efforts by the Customs Service to establish a container security regime that will effectively conduct security screening of containerized cargo at the foreign port of loading, rather than the U.S. port of discharge. The Council and its Member lines are working diligently with Customs to implement the new advance cargo declaration filing requirements in as smooth and effective a manner as possible. The Council and its Member lines have strongly supported the U.S. government's successful initiative, led by the Coast Guard, at the International Maritime Organization to establish a new international security regime for vessels and marine terminals. The Council has supported the Coast Guard's requirement that vessel Notices of Arrival be filed 96 hours in advance of arrival in a U.S. port. The Council has worked with the Coast Guard and the Immigration and Naturalization Service in support of a single, effective advance reporting system for all crew members aboard vessels calling in the United States. The

Council has participated in numerous meetings of the Container Working Group, referred to in the Federal Register notice and co-chaired by the Department of Transportation and the Customs Service, in the effort to develop transportation security enhancement recommendations. The Council is participating in and supporting the efforts of the U.S. government at the World Customs Organization to develop effective international cargo security requirements.

The Council has a strong commitment to enhancing the security of America's trade, and a record of supporting the government's efforts in this regard. In that vein, the Council also supports the objectives stated in the Federal Register notice of November 20, 2002 regarding Operation Safe Commerce (OSC). We also strongly support the Executive Steering Committee providing clear oversight and guidance to the OSC effort. Sound and clear guidance from both the load centers and the Steering Committee will be needed to ensure that these federal dollars are spent prudently on projects that will effectively examine security gaps and meaningfully evaluate ways to effectively meet the government's defined security requirements. We agree with the Federal Register commentary that OSC can provide an important "virtual laboratory" for evaluating security solutions. A laboratory's results, however, require some scientific method and controls for the experiment's results to have validity and credibility.

I. Vulnerability Assessments and Definition of Requirements

The OSC process should begin by a careful and clear analysis of the security gaps and vulnerabilities in the present cargo supply chain. The three load centers that will coordinate these OSC projects can certainly participate in this process; however, it would seem unlikely that in today's world of intermodal containerized shipping, systemic security gaps or vulnerabilities are likely to be substantially different between Asia-U.S. trades and Europe-U.S. trades, for example, or be substantially different among the three load centers themselves. Asia-Los Angeles commerce and Asia-Seattle commerce are not that different. The point here is that it would be helpful if the three load centers and the Steering Committee managed a program that operates from a common vulnerability and risk analysis, a common set of priorities, and a common set of objectives. This is not to say that value cannot be derived from different projects from the different load centers, but to suggest that there should be some common foundation, approach and objectives in these projects, and that the foundational security gap analysis should be done in close coordination with the responsible federal agencies. In this regard, we recommend that the OSC projects receive the benefit of guidance from the Steering Committee specifically identifying the most important problems and needs it believes the submitted projects should address.

Once these priorities are selected by the Steering Committee, after being developed and presented by the load centers, we see the role of the ocean carriers coming clearly into play. We recommend that this role would be to assist the load centers in developing thorough proposals that address the prioritized list of security gaps and vulnerabilities. Once developed, the carriers would be able to play a dedicated, informed

and committed role in the testing and evaluation of these initiatives in the "virtual laboratory". The ocean carriers would be able to bring not only their vessels, port facilities and equipment to these testing venues, but also their end-to-end transportation networks.

OSC clearly envisions evaluating a number of different kinds of products, ranging from cargo information systems, to seals, to sensors, to tracking devices. It would seem appropriate that the funded projects should be evaluating such new technologies based on whether they meet specifically identified security gaps and requirements, and they should evaluate the product not just in isolation, but in comparison to other means of achieving the same security objective. If OSC projects simply become a forum for technology vendors to show whether their products operate in a commercial setting, an opportunity to evaluate security enhancements in a meaningful manner may be lost. We believe there is a need for the development of standardized test protocols to be used in the projects so that meaningful and reliable comparisons and evaluations can be made amongst the projects.

For example, it is understood that OSC will be testing electronic seals. When that is done, what measures and criteria will be used to evaluate whether the electronic seal has met the objective of the OSC process? Will the project also simultaneously test manual high security seals so that an assessment can be made regarding what security protection an electronic seal provides that a high security manual seal does not? If such an assessment is not done, what would be the value of the exercise?

For example, the Federal Register notice indicates that information management systems may be tested. Will the evaluation of such information management systems take into consideration how such systems may relate to existing legal requirements regarding who must submit what information to the government when, and how such systems might relate to existing government information systems and data analysis?

In short, the OSC projects should be focused and well-structured, and selected on the basis that they attempt to effectively address and evaluate clearly understood security issues and possible solutions, not just particular products.

II. Criteria for Projects

1. *Validate Security at the Point of Origin:* We strongly support this first criterion. Ensuring that containers do not have security risks loaded into them in the first place is the most important element of a secure supply chain, because without that, the other measures discussed can only monitor or secure an assumption of security, not the fact of security. To the extent OSC projects can contribute improvements to security in this area, they will be contributing to addressing a most difficult challenge.

2. *Secure the Supply Chain:* We support this criterion and the objective, as evidenced by the fact that all Council Member lines have applied to participate in the C-TPAT programs, which has this as its objective. We would note, however, that the criteria as

stated is so broad as to give little specific guidance regarding what kind of projects are of interest to the Steering Committee.

3. *Enhance the Accuracy and Communication of Cargo Information:* We support this criterion and support test projects that could determine how better cargo documentation requirements might enhance supply chain security, but believe further clarity and definition of intent could be helpful. The transmission of cargo information today is regulated by law and administered by federal agencies. The Customs Service is a major and very active regulator of this information and is in the midst of implementing a major new advance cargo declaration-filing regime. We have no objection in principle to OSC projects that may better meet the government's goals in this regard, but believe such projects could be a waste of effort and money unless they are conducted with some understanding of the government's specific goals and requirements. In this regard, we would request that the Steering Committee, especially the Customs Service, provide appropriate guidance.

4. *Monitor the Movement and Integrity of Cargo in Transit:* We support this criterion, but have some concern that the way it is phrased presupposes that technology will provide superior security before that is actually tested and evaluated, and assumes that certain devices may be needed without clearly establishing and obtaining agreement on the security gaps and requirements that the device is supposed to address.

For example, the criterion provides the example of GPS transceivers as a device to be tested, yet it is unclear what the OSC project goal should be for a project involving GPS devices. There are more than 12 million containers in use today. Will OSC projects evaluating GPS devices be narrowly focused on the issue of does a particular GPS device work when attached to a container, or will they be designed to analyze and evaluate not only whether a particular product may "work", but what would be involved in their application and deployment to the world container fleet and what security enhancement would actually result from such an application? This relates to the point made in Part I of these comments about the importance of identifying the security goals, gaps and requirements to guide OSC projects.

Similarly, we have no objection to the testing and evaluation of electronic seals, but believe that if such OSC projects are to have probative value, they should simultaneously test and evaluate high security manual seals so that a comparative assessment can be made of whether and how an electronic seal provides a level of security protection that meets agreed-upon security requirements more effectively and more reliably than "off the shelf" non-electronic devices. We also would urge that, as OSC projects test and evaluate seals, the analysis of the sealing issue be comprehensive and not just focus on whether a device operationally does what its manufacturer says, but also addresses what would be required for a device to achieve its potential if it were to be used on containers deployed around the world.

5. *Other Criteria:* The objective of the fourth criterion – to lessen the susceptibility of a container shipment from being compromised once it has begun its transit -- is certainly a

worthwhile goal. The first criterion recognizes that in protecting against the risk of terrorism, one must not focus only on the possibility that a terrorist might intercept a container in transit, place something in it, and reinsert the container into the flow of commerce with the hope that it would not be detected, but the potentially more likely risk that a terrorist would place something in a container at the container loading origin, affix a seal and any other required device, and send the shipment on to its destination. We see nothing in the OSC project criteria that encourages OSC efforts to test or evaluate more effective or efficient technologies for the non-intrusive inspection of containers. These technologies answer a security question of paramount interest -- What's in the container? -- and we would encourage OSC to actively promote further advancement in this area. After all, at best, seal anomalies or data anomalies only indicate that there may be a reason to inspect a container, yet there is nothing in the proposed criteria that tries to encourage the development of improvements in container inspection technology.

III. Development and Evaluation of OSC Projects

It is unclear how OSC projects will be evaluated. As it is also still uncertain how shippers and carriers will be involved in the OSC projects to be submitted by the three load centers themselves, we believe it is important that the Steering Committee express its commitment to establish an open transparent process involving shippers and carriers in the evaluation of the OSC projects and in the assessment of any possible recommendation that may result from them.

We would like to offer an additional observation in this regard. Effective implementation of many of the potential security enhancement that may be evaluated pursuant to Operation Safe Commerce will depend upon their international acceptability. For example, any device that utilizes radio frequency spectrum must have its bandwidth available and approved for such use in the various nations in which containers are transported. For example, procedures and protocols to ensure secure stuffing of containers at shipments origins will require the cooperation of foreign governments. The Council would like to encourage the Steering Committee to give serious consideration to how best to keep foreign governments informed about the OSC process, and possibly to provide for the participation of interested foreign governments both in some of the OSC pilot projects and in their evaluation. Similarly, there should be value -- as part of the evaluation of the results of the OSC pilot projects -- in obtaining information about lessons learned and experiences gained in pilot projects for enhancing the international supply chain conducted by other countries.

The international dimension of supply chain security is particularly important in view of recent international initiatives. For example, the G8 Summit in Canada last June agreed to a U.S. sponsored action plan on transportation security that, inter alia, commits the G-8 countries "to develop, in collaboration with interested non-G8 countries, pilot projects that model an integrated container security regime". Also under American leadership, the recent APEC Summit launched the so-called "Secure Trade APEC Region (STAT)" initiative that is intended to complement the G8 transportation action plan and

the “smart border programs” with Mexico and Canada. This initiative, inter alia, aims at “identifying and examining high-risk containers, assuring in-transit integrity providing advance electronic information on containers to customs, port, and officials as early as possible in the supply chain”. We are also aware that the European Commission has commissioned a project for the end-to-end tracking of shipments between Europe and the United States. This project, known as the “Safe InterModal Transport Across the Globe”, or SIMTAG, was presented to the 5th Forum on Intermodal Freight Transport in Europe and the United States in April 2002 and, as a result, the U.S. Department of Transportation was invited to observe the implementation and results of SIMTAG.

The conclusions reached from well-done OSC evaluations are likely to receive more favorable consideration from other nations that would have a direct interest in their implementation if the process used is inclusive and open.

IV. Conclusion

Ocean carriers recognize the challenges in more effectively securing international commerce, and are committed to continue working with the government to achieve that objective. The Council and its Member lines are prepared to participate in OSC projects and hope that those efforts, and the comments above, will be of assistance in meeting these goals.