CARGO, CONTAINER AND SUPPLY CHAIN SECURITY – Challenges and Priorities
HEARING QUESTIONS
2 April 2008
10: 00 AM – Panel 1

Questions for the Record

For Christopher Koch

Questions for the Record Submitted by the Chairman The Honorable David Price

COST SHARING AND BURDEN SHARING

QUESTION: *Please provide your views of the appropriate form of cost- and burden-sharing that could or should be borne by the private sector – among shippers, carriers, port operators and consumers – to establish the kind of security system required to protect our supply chain.*

- *What kinds of processes and adaptations are going to be required on the part of the private sector? What kind of role should the private sector take in designing and implementing security?*
- *What are the prospects for achieving a system where the cost of screening is either shared by the private sector, or fully privatized?*

RESPONSE: Under the various regulatory regimes that the government has established and applied to the private sector to enhance supply chain security, there are a variety of costs and burdens that the private sector bears. For example, ship and port facility operators have incurred billions of dollars of costs to comply with the ISPS Code and the Coast Guard's maritime security requirements. Ocean carriers and NVOCCs incur costs in providing Customs and Border Protection (CBP) with advance manifest data. Importers and ocean carriers will incur additional costs in complying with CBP's "10 plus 2" regulations when they become final.

By and large, the resultant cost and burden sharing are derived from the classic government regulation model – the government incurs some costs for implementing its portion of the obligations, and the private sector incurs some costs for its implementation and compliance with the various regulatory obligations. So long as the regulations developed are well reasoned, lead to meaningful and tangible enhancement of security, and are developed with care with respect to the costs and obligations that would result, this model generally works satisfactorily.

Voluntary programs to improve supply chain security, such as Customs' Trade Partnership Against Terrorism (C-TPAT) operate in a similar manner. In this case, CBP establishes particular objectives and works with the private sector to develop program elements that are to be implemented in order to participate in the program. Unlike regulations, a private sector participant can withdraw from a voluntary program at any time that the costs become unreasonable. To date, that has not occurred, even though the costs can be significant to establish, implement, monitor and validate participation in such a program.

In the end, every new program or regulatory initiative will result in costs for the private sector and costs for the government. The existing allocation of costs would appear to be a reasonable and fair allocation. The key is to ensure that the programs in fact have significant value in enhancing supply chain security. It is also essential that the private sector not be tasked with law enforcement functions, which must remain a governmental function.

Another factor affecting U.S. international supply chain security initiatives is that they can and do impose costs on foreign governments. Many governments have worked cooperatively with the U.S. Coast Guard and CBP and expended their own resources in such efforts. However, not all foreign governments see the issues and the priorities the same way as the U.S. government may see them. There are times, particularly when the U.S. government establishes a policy affecting a foreign government without adequate consultation, that such governments may question their value.

The final part of the question presented above relates to container "screening". In order to be clear, a distinction should be maintained between container "screening" and "scanning".

"Screening" is the process used by CBP to review advance information about a containerized cargo import shipment and perform risk assessment, before it is loaded on a vessel in a foreign port. The private sector incurs certain costs both in complying with the regulations mandating advance information filing with CBP, and the delays that may result from CBP's decisions to stop and/or inspect a container. CBP incurs costs in running the National Targeting Center that receives and analyzes the data required from the private sector and other sources of data, including classified intelligence information, that are used in targeting. Cargo "screening" is a function that is clearly a sovereign function of the government. It does not appear reasonable to believe that such a function could be privatized.

Container "scanning" is the process of obtaining data about containerized cargo shipments from radiation scanning and non-intrusive inspection (NII) scanning technology. This has been and continues to be a sovereign function of the government.

If the Congress and the Administration wished to consider "privatization" of this function, a serious and careful analysis of a number of significant issues would be required. It is difficult to see how this scanning function could be fully privatized. For example, resolution of radiation alarms would appear to require sovereign authorities. For example, analysis and action based on review of NII imaging would appear to require sovereign authorities.

Some have raised the possibility of what might be called a "partial" privatization of the container scanning function. This is generally understood to envision overseas marine terminal operators' purchasing, installing and operating radiation and NII container scanning equipment, charging each container a fee for "scanning" them, and providing the resultant data and images to government authorities. As the Council has noted on several previous occasions, such a concept would require Congress and the Administration to address a number of significant issues that current law and policy do not address, including the following:

1. Such an initiative would require the consent of the foreign host government, and compliance with any conditions that the foreign government were to impose on such operations. For example, would the government in Hong Kong agree that such an enterprise should be established at its port facilities?

2. The Congress and the Administration would need to consider and decide what criteria a foreign company would need to satisfy in order to be trusted to perform this function. The development of this criteria would need to be both careful and transparent given the sensitivity and implications involved in the U.S. government approving one foreign terminal operator and not another. For example, would the Congress find Dubai Ports World and Hutchison Whampoa, two of the largest terminal operating companies in the world, acceptable to perform these security functions?

3. The government would need to be clear about the technical standards the scanning technology would need to meet (e.g., reliability of detection, false alarm rate, functionality, etc), as well as equipment operating and maintenance requirements. Further, would these standards be adopted as international or U.S. standards? If U.S. standards were required, how would such standards be imposed?

4. To privatize this function, marine terminal operators would probably need the government to require this scanning service to be performed. Without a requirement that the foreign marine terminal operator perform this action, it would likely not be able to impose this service on containerized cargo and make a financial profit on the enterprise, because there is no market demand for the service to justify the investment in such equipment. The government would thus have to create the market demand via a mandate that this function be performed.

   This, however, raises a question that so troubles the present statutory provisions of the "9/11 Commission Recommendations Act" regarding 100% container scanning, namely how as a practical matter can the U.S. government require such activity by foreign enterprises? The jurisdiction to impose such requirements on foreign terminal operators lies within the sovereignty of the various foreign nations, which have very different views on this issue.

   For example, the European Commission earlier this month provided formal comments to Customs and Border Protection on the 100% container scanning concept, stating: "we fundamentally disagree with the 100%

scanning approach and we do not contemplate 100% scanning in Europe." A copy of the European Commission's comments on this subject is attached as an Annex to these responses to the Committee's questions.

5. The government would need to recognize that, while some terminal operators might derive a financial profit from running containers through such scanning equipment if cargo were required to be scanned, other terminal operators may be forced to absorb all or a portion of the related scanning costs based on the competitive marketplace in that geography, and be unwilling to take on this function. In both cases, the functions the terminal operator would perform need to be clearly defined and agreed, but they would also be limited. They certainly would not constitute a full privatization of the functions or the costs of such a mandate. For example:

    a. Such operators are not candidates for performing the security analysis or security resolution that such technology requires. They also would be unlikely to assume this role or this liability. The functions of information security analysis and response protocols would require the participation and resources of foreign governments and CBP.

    b. The government would need to have a clear strategy for what it would do with the data and the images that foreign terminal operators would send it for millions of containers a year. While the concept of such a "partial privatization" might be financially profitable for some terminal operators under certain circumstances, and could relieve the government of the costs of the purchase and operation of the scanning equipment, it would still impose substantial costs on the U.S. government and on the trade community. Those costs would include data transmission costs, CBP personnel to analyze the data and NII images generated, the resulting charges to American import cargo, and the delays that the technology will routinely cause to certain types of cargo. Further, such a system would impose similar, substantial costs on the host governments that would need to be understood and agreed.

6. If the Congress and Administration were to decide that not every import containerized cargo shipment needed to be run through NII scanning technology before vessel loading, but only those that CBP's targeting system determined justified such inspection, then the financial returns to the terminal operator would change, as it would not derive revenue from every container it handles but only those that are considered to present some kind of risk. How that would affect the possibility of "partial privatization" would require further consideration. We would note, however, that the trade community would likely have legitimate concerns about resolving this question by requiring every container to be subjected to a charge for NII scanning even if the government did not in fact analyze the resulting data.

7. The issue of "partially privatizing" container scanning would, like the statutory provisions of the "911 Recommendations Act" on 100% container scanning, require an assessment of how such a mandate could be reasonably applied to transshipped cargo. One cannot fairly compare operations in Hong Kong,

where containers generally arrive through a terminal gate and can be scanned there, with port operations in Singapore, where most containers do not arrive through a gate and where container scanning would be much more complicated.

8. The issue of how a 100% container scanning mandate could be implemented, even through a partial privatization, in small and poorer ports, such as in the Caribbean, remains an unaddressed and unresolved issue.

9. The issue of how a 100% container scanning mandate would be implemented, even through a partial privatization, at U.S. port facilities on outbound U.S. export cargo (i.e. the expected and predictable demands that foreign governments would likely make for reciprocal action by the U.S.) remains an unaddressed and unresolved issue, and is further complicated by questions about whether American labor would be willing to drive through the NII container inspection equipment.

10. We note that some terminal operators in some ports, which handle light cargo that does not contain natural radiation and which is more easily subjected to NII scanning analysis (like Hong Kong), may be more interested in participating in such a concept than terminal operators in ports that handle dense cargoes of earth products that emit natural radiation (like the Mediterranean).

In summary, there is no way to assess the prospects for even a "partial privatization" of this container scanning function unless the Congress and the Administration have a public dialogue and provide much greater clarity on such important strategy questions.

INTERNATIONAL STANDARDS

Question:

- *What is your assessment of efforts to internationalize CBP container security programs through multilateral agreements, standards and the like?*
- *What recommendations would you make for DHS or the U.S. government to help work towards an effective international norm for dealing with supply chain security?*

Response: CBP faces a difficult challenge in its efforts "to internationalize container security programs through multilateral agreements". The U.S. Coast Guard can work through the International Maritime Organization (IMO) to internationalize ship and port security via mandatorily applicable rules and standards that are binding on IMO member states. In addressing cargo security at the international level, CBP works through the World Customs Organization (WCO), which unlike the IMO, cannot make decisions that bind member states.

This is not intended in any way to denigrate the WCO or its efforts to address supply chain security. Nor is it intended to reflect a lack of importance regarding CBP's efforts at the WCO to develop a voluntary international supply chain security

framework. It is simply to point out that the WCO, even if agrees with CBP, cannot impose a result on member states, even when there is agreement within the WCO.

Not all customs administrations around the world view supply chain security with the same perspective as the United States government. Some governments do not perceive the same threat to cargo security. Some governments do not have the resources or capabilities that CBP has to address the threat. Expecting international agreement or mandatory uniformity regarding supply chain standards that would meet the requirements of CBP and the Congress is optimistic at best.

It seems reasonable and prudent for CBP to pursue international agreement and consensus wherever possible, whether that is through multilateral or bilateral agreements, but to have realistic expectations.

As to the development of standards, the International Standardization Organization (ISO) can play a useful, supportive role for some of CBP's container security programs. For example, the ISO is finalizing its mechanical seal standard that is referenced in CBP's C-TPAT program and in statute. For example, the ISO has recently published amendments to its standards for the construction and testing of maritime containers to address vulnerabilities, identified by CBP, regarding the traditional door handle seal location.

The ISO, as a private organization, however, can not be given supply chain security responsibilities that rightfully belong to governments. The identification and definition of objectives, needs and requirements for supply chain security are government functions that – as is typically the case regarding CBP's programs – are exercised upon consultations with the business community. However, once such objectives, needs and requirements have been identified by governments, the ISO may assist in providing guidance in the development and implementation of technologies and processes. International standards developed through the ISO may help ensure interoperability and compatibility of technologies regarding e.g. frequencies, reader infrastructure and communication protocols (issues that would also be relevant for the viability of any future decisions regarding more prevalent use of CSDs as discussed below in response to the question regarding CSDs by Congressman Rogers). Also, devices built according to international standards would not need to be certified and approved by each government -- something that obviously is very important for containerized shipments that are being transported internationally.

Questions for the Record Submitted by the Honorable Harold Rogers

QUESTION: *Please provide the WSC's views on the usage of a container / conveyance security device (CSD) on shipping containers.*

RESPONSE: CBP has announced that it plans to conduct various pilots that will test "conveyance security devices" in a number of different settings where they may provide

useful information. The Council supports the agency's efforts in this regard, because these kinds of devices are not "miracle cures" and their limitations as well as their potential benefits need to be carefully considered and tested.

Some of the questions include the technical requirements for such devices. CBP has issued specifications for RFID technology devices for their initial pilots. These and future specifications must address issues such as: what specifically the device would be required to do and its security value. Thus, for example, the device specifications for the CSDs being piloted only require that the device report on whether the right side conveyance door has been opened; they definitely do not detect what the contents of a container are, or whether there has been a breach of the container through the top, bottom or sides of the conveyance.

Other questions that will need to be addressed include: what acceptable false positive and false negative reading rates would be[1], what radio frequency would be used, the requirements for the installation and operation of the necessary device reader infrastructure, the requirements applicable to the necessary communications interface and protocols with CBP, the security vulnerabilities of such devices,[2] the necessity of interoperability of various vendors' devices and systems, the data to be captured and transmitted by the device, identification of who will have access to the data in the device, survivability and vulnerability of the device, power or battery life requirements, the probability that the device can be detected or removed without detection, required data messaging formats, event logs, and data encryption.

These questions are even more complicated in the environment of international maritime commerce than they would be in a more controlled environment of U.S. border stations where CSD reading infrastructure and response protocols would be under the sole control of CBP.

Finally, the operational protocols that would be needed for effective use of such devices need to be analyzed and considered. Every time a container door is opened, a CSD will alarm; however, many container door openings do not create security risks. There are legitimate operational reasons that justify opening the doors. For example, in some trade lanes, foreign Customs authorities will open the doors of most containers before they leave the country, meaning that virtually all containers from such locations would alarm if equipped with CSDs. What operating protocol would be applied in such situations?

In short, the CBP pilot programs will begin to shed some useful light and analysis on a wide array of questions that would have to be addressed in considering the application of such technology.

It is also worth noting that, as of October 2008, every U.S. import containerized cargo shipment will need to have an ISO standard security seal affixed to it, addressing some of the concerns that a CSD seeks to address.

---

[1] The 4% error rate permitted under the CSD specifications for the CBP pilots would be totally unacceptable for wide-spread commercial application.

[2] For example, the World Shipping Council in its work on developing an international standard for electronic seals noted the security vulnerability that can be created when such devices have a "read/write" capability that allows data in the devices to be written and amended. The equipment that allows one to write and amend data in a CSD (generally a hand held device) thus can become a potential security vulnerability.

Questions for the Record Submitted by the Honorable Robert Aderholt

QUESTION: *Mr. Koch: Textile transshipment is a major issue for my constituents, many of whom manufacture socks. I have heard that transshippers use various means to conceal their cargo, including using false bills of lading, not affixing country of origin labels, and using third-country transit routes. What has private industry done to try to prevent this practice? What do you think can be done in the future?*

RESPONSE: CBP has designated imports of textile and apparel products as a "Priority Trade Issue" for 2008. CBP has noted the following information:

> Different schemes are used to evade duties or quotas on imports of such goods. Some importers engage in improper transshipment, while others use false documents or labels or provide incorrect descriptions of the merchandise. In recent textile enforcement operations over $12 million in misdescribed goods have been seized. CBP has also identified significant intellectual property rights violations involving textile products and seized approximately $27 million in infringing goods in 2007.
>
> CBP uses a multifaceted approach consisting of trade pattern analysis, on-site verification, review of production records, audits and laboratory analysis to enforce U.S. trade laws and ensure that the appropriate revenue is collected. To conduct on-site verifications, CBP's Textile Production Verification Teams travel to foreign factories to review and verify that wearing apparel that is shipped to the U.S. is produced at those facilities. These teams visited 15 countries and approximately 671 factories in FY 2007, a 57 percent increase over the previous year.
>
> Import specialists with specialized commodity knowledge analyze and review textile imports for possible violations. CBP has seized more than $100 million in goods since the beginning of 2006 and close to $50 million in 2007 for violations of the China quota agreement. In addition, CBP issued 68 penalty actions valued at $50.1 million. More than 13,000 physical examinations were performed, 1,527 fiber samples were analyzed by CBP labs and 66 audits were conducted.

The Committee may wish to obtain further information from CBP on these efforts.

In order to bolster CBP's efforts to track transshipped cargo, ocean carriers have agreed as part of the C-TPAT program: "Bill of lading information filed with CBP should show the first foreign port (place) where the sea carrier takes possession of the cargo destined for the United States." Thus, an ocean carrier will not knowingly participate in an improper transshipment that tries to disguise the origin of the cargo shipment. What an ocean carrier cannot detect, however, is a situation where a shipper has a container transported, for example from China to Singapore, and then rebooks the cargo to the U.S. in a new container with a different carrier.

Ocean carriers will cooperate with CBP in its law enforcement efforts whenever they are requested to do so by the agency.

In addition, we would note that the pending “10 plus 2” rulemaking by CBP would give the agency important additional targeting data and tools earlier in the transportation process, which could enhance the agency’s ability to detect illegal cargo movements and improper transshipments. That rulemaking has not been finalized, but the World Shipping Council supports it.

###