



November 5, 2007

The Honorable Bennie G. Thompson  
Chairman  
House Homeland Security Committee  
H2-176 Ford House Office Building  
Washington, D.C. 20515-6480

Dear Mr. Chairman:

At the Committee's October 30<sup>th</sup> hearing on maritime security and the SAFE Port Act's implementation, the issue of "container security devices" (CSDs) was raised. Discussion at the hearing implied that CSD technology was available and ready for widespread application to international maritime containerized traffic. We would like to take this opportunity to explain why this is not the case and to identify issues that have not been addressed with respect to the application of such technology to international maritime commerce.

First, there is no agreement regarding what constitutes a CSD. For example, some say that a seal is a CSD; some say a seal is not a CSD. For example, is it sufficient that a CSD monitors one container door only as the GE device referenced at the hearing does, or must a CSD monitor both doors? For example, must a CSD detect intrusion through the sides of a container?

Second, if such devices were to receive widespread use in international commerce, it is essential that there be internationally developed and agreed, non-proprietary standards and requirements for such technology. No such international standards or requirements exist today. The government has not issued even draft requirements which could form the basis for the development of standards.

Earlier this year, the Department of Homeland Security's Science and Technology directorate prepared an 82 page draft set of technical requirements for container security devices and the operating protocols associated with such devices; however, that drafting effort is undergoing further review within the Department. At the same time, the European Union, China, Japan and South Korea are experimenting with different container security technology that may not be compatible, let alone interoperable, with various devices that Committee members may have seen.

The Council and other members of the trade have requested that DHS allow for

full transparency into the development of this effort and solicit public comments on any draft requirements, after they have completed internal government review.

What is it that must be addressed before CSDs could be considered for widespread use and why are agreed standards necessary? The answer is that there needs to be a common definition of:

- What the device would be required to do?
- Is a particular technology to be used, such as RFID or satellite-based, and if so, which one?
- If RFID technology is to be used, what is the radio frequency for the device and is it internationally accepted and available for commercial usage? Many countries either restrict the frequency bands for commercial deployments or impose licensing requirements for such deployments. Different vendors are proposing different frequencies. For example, GE's proposed frequency is different from Lockheed Martin's. We know from our involvement in other international standard setting activities that none of these frequencies can be said to be unconditionally available in all trading nations in the world.
- What are the acceptable false positive reading rates? A false positive rate of 2% would create roughly a quarter of a million containers arriving in U.S. ports that would need to be inspected for no reason.
- What would acceptable false negative reading rates be?
- How easy and how long would it take to defeat the device, i.e., an adversary opens the door of the container in such a way that detection is bypassed? We understand that some work in this area has been performed by U.S. government laboratories with disappointing results with regard to some of the CSDs being considered.
- Where do such devices make no sense to use? For example, it is very common that many, if not most, containers leaving many Central American ports will have been opened and inspected by local Customs authorities. What good would CSDs do in trade lanes where container doors are customarily opened as an accepted or required part of the transportation of the goods?
- What would be the requirements for the installation and operation of the necessary device reader infrastructure? If RFID technology is used, such infrastructure would need permission to be installed at privately operated facilities around the world.
- What are the requirements applicable to the necessary communications interface of the device CSD reading infrastructure with Customs and Border Protection (CBP)? What are the operational and response protocols with CBP? This is a critical set of questions.
- What are accepted security vulnerabilities of such devices? For example, some CSDs allow any person with a handheld reader to interrogate the device and amend and delete data in the device. How is this vulnerability to be addressed?
- In the absence of internationally developed and agreed, non-proprietary standards, how would a CSD system ensure the necessary interoperability of various vendors' devices and systems? Proprietary systems would face substantial resistance from users, would result in duplicative and redundant investments in reader infrastructure, and would create confusion amongst the

users regarding the capabilities and functionalities of different types of devices, possibly leading to sub-optimal deployment results.

- What is the data to be captured and transmitted by the device?
- Who will have access to the data in the device, and who will own and control the data that is generated?
- What are the survivability requirements of the device, and the power or battery life requirements? Would the usage of container scanning equipment reduce the functionalities of the devices?
- What is the probability that the device can be detected or removed without detection, thus defeating the entire purpose of the device?
- What are the required data messaging formats, event logs, and data encryption requirements?
- What impact would device-equipped containers have on the safe operations of container vessels, including their radar and navigational aids, and would they have any impact on shore-based equipment and operations in ports and terminals?

These questions are not simple, but they cannot be avoided by either the vendors who would like to sell these devices, by the thousands of maritime commercial operators who would need to install and operate the device reading infrastructure in countries around the world, or by the government who needs be an integral part of the use of such devices. Nor can these questions be dealt by the United States alone. Maritime containers move internationally, and any solution identified as meeting identified and agreed requirements would need to be embodied in international standards that provide for open architecture, non-proprietary competition and deployment.

The Council believes it is essential, if an interest in CSDs is to be pursued, for the government to undertake a fully transparent and very clear articulation of its draft views on the requirements for such technology and the related operating systems and protocols, and to provide the public with a meaningful opportunity to comment upon such draft requirements, *before* they are advanced as an element of the government's container security strategy.

When the Congress enacted the "9/11 Commission Recommendations" legislation, it provided for a helpful clarification of the SAFE Port Act. Section 204(a) of the SAFE Port Act had provided: "Not later than 90 days after the date of enactment of this Act, the Secretary shall initiate a rulemaking proceeding to establish minimum standards and procedures for securing containers in transit to the United States." It was not evident what this provision meant or how it might be interpreted, and the section's time deadlines were not going to be met.

Accordingly, Congress amended this section in the 9/11 Act by providing that:

"(B) Interim Requirement.-- If the interim final rule described ... is not issued by April 1, 2008, then .... effective not later than October 15, 2008, all containers in transit to the United States shall be required to meet the requirements of International Organization for Standardization Publicly Available Specification 17712 standard for sealing containers...."

Thus, by next October, all U.S. inbound containers will be required to have ISO standard seals.

In addition, we note that Customs and Border Protection has indicated that it plans to undertake pilot usage of certain container or trailer security devices under defined and controlled circumstances, such as along the U.S.-Mexico border, where CBP would control the border crossing and the device reading infrastructure, and where selected secure facilities would test the devices on trailers that would have no reason to be opened prior to crossing the border.

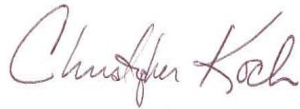
We believe such a controlled and judicious pilot program by CBP has merit.

We believe, however, that CSD application to international maritime commerce currently has too many unaddressed questions to be considered appropriate for widespread application.

If the Committee has any further questions about container security devices, the Council would be pleased to try to be of assistance. We respectfully request that this letter be made part of the record of the Border, Maritime and Global Counterterrorism Subcommittee's October 30<sup>th</sup> hearing.

Thank you for your consideration.

Sincerely yours,

A handwritten signature in red ink that reads "Christopher Koch". The signature is written in a cursive, flowing style.

Christopher Koch  
President

cc: The Honorable Loretta Sanchez  
The Honorable Peter King  
The Honorable Mark Souder  
The Honorable Gus Bilirakis  
The Honorable James Langevin  
The Honorable Henry Cuellar  
The Honorable Daniel Lungren  
The Honorable Al Green  
The Honorable Michael McCaul