

January 2005

## **Cargo Security Strategy**

**Dennis L. Bryant**

The U.S. Department of Homeland Security recently released its draft White Paper on a National Cargo Security Strategy. The Department is seeking stakeholder feedback. The vision is for “a system for supply chain security that mitigates the evolving terrorist threat and facilitates the free flow of global commerce in order to ensure the physical and economic well being of the United States and its trading partners.”

The White Paper is a long-belated and somewhat half-hearted attempt to mend fences and appear to be moving forward, while expending little new capital. The paper runs on for nine pages, offering no new ideas and making few commitments. It has the appearance of an uneasy political compromise between feuding federal agencies.

The one clear commitment is found on page eight, where it says the Department “will, as a short-term step, mandate the use of high security mechanical seals on all in-bound containers.” There is, as yet, no official government standard as to what constitutes a high security mechanical seal. While there is a recently-developed ISO standard on this topic, it is unclear if qualifying seals are being produced in sufficient numbers to meet the projected need.

The remainder of the White Paper is vague, talking about enhancing the physical security of the supply chain, leveraging federal resources, pushing out the border, and working with the international community without really explaining how. The document itself is what the State Department would call a “non-paper.” It is marked “Draft”. It bears no letterhead or other indication that it is an official DHS document. It was distributed at a forum sponsored not by DHS, but by the Homeland Security Institute. It talks about seeking industry feedback, but provides no points of contact or addresses to which comments can be submitted. The term “plausible deniability” comes to mind.

The concept with which DHS is laboring is – at its heart – fairly direct, although the execution is extremely difficult. There are three basic elements: (1) the authorities must know what is entering the system, where entry is being made, and who is responsible for the entry; (2) the authorities must know that the cargo is secure during transit; and (3) the authorities must know when the shipment is complete, so that it can be deleted from the active system.

E-mail

[dennis.l.bryant@gmail.com](mailto:dennis.l.bryant@gmail.com)

Internet

<http://brymar-consulting.com/>

Maritime Reporter & Engineering News

<http://marinelink.com/en-US/magazines/Archive.aspx?MID=3>

For intermodal containers, this means knowing what is being stuffed into the box, where the box is being stuffed, and who is doing the stuffing. The White Paper briefly discusses the need for information at the point of box stuffing. It then indicates that meeting this strategic objective requires the rapid build-out of the Automated Commercial Environment (ACE) platform, being developed by Customs and Border Protection (CBP). The problem is that ACE was designed in the pre-9/11 era and is not intended to capture box-stuffing information. Express package companies, such as UPS, already track their items electronically from pickup to delivery. A similar approach, but admittedly more complex, could be used for cargoes generally.

The current dumb box is inherently insecure. There is an Internet site showing how to remove the doors from a container without disturbing the seal, just by jimmying the hinges. There have been cases where goods have been inserted into (or removed from) a container by going through the floor. Until a secure, tamper-evident container has been developed and deployed, putting a high security mechanical seal on the door only deters amateurs and creates a false sense of security. Installation of GPS transponders (like those placed on many trucks) should also be considered. Access could also be provided for insertion of sensor probes to detect anomalies.

The use of non-intrusive sensors should be significantly increased. Detectors utilizing the entire electro-magnetic spectrum (x-rays, gamma rays, infrared, radiation, etc.) are available, but expensive. Personnel to operate the devices must be employed and trained.

Current programs, such as Operation Safe Commerce, the Customs-Trade Partnership Against Terrorism (C-TPAT), and the Container Security Initiative (CSI), were a good first step. Follow-through, though, has been lacking. C-TPAT was advertised as providing participants with expedited handling of their cargoes upon arrival in the United States. CBP is unable, though, to demonstrate that C-TPAT cargoes receive preferential treatment. Operation Safe Commerce seems to have stalled. These programs have not been coordinated and potential synergies have been lost.

I do not, by these comments, mean to imply that the cargo security problem is easily solved. I do mean, though, to say that the White Paper employs far too much bureaucratic language and leaves one with the impression that we just need to let the government finish what it has started. In some instances, there are excellent government initiatives that promise to bear fruit. In other areas, though, the government needs to have meaningful dialogues with other stakeholders in order to just figure out the problem, let alone coming up with a viable solution. Having a private group host a two-day meeting in Washington, DC on cargo security is not the end of the process. It is only just the most basic beginning, and was long overdue.