

Container Port Security: A Layered Defense Strategy to Protect The Homeland and The International Supply Chain

WENDY J. KEEFER

INTRODUCTION

The events of September 11, 2001 aimed a spotlight on the true state of our national security. Though that particular terrorist attack utilized airlines, the lack of any real security measures at U.S. seaports raised perhaps even greater concerns. Ports provide entry from all over the world into the United States. People and cargo arrive at U.S. ports with relatively little oversight. Once there, via road, rail or otherwise, they may travel throughout the country.

Recent government initiatives to tighten port security create numerous layers of protection from the entry of dangerous individuals and cargo. This layered defense seeks to prevent future attacks upon the country, as well as to protect the international supply chain. Disruption of trade via attack on or at U.S. ports would be economically devastating.

Port security, however, is not a unilateral endeavor. It involves all levels of government, private domestic and international businesses, and foreign governments. Also, it encompasses numerous issues—from the security of actual port facilities to passenger identity verification to threats posed by container cargo shipments. Prior to post-9/11 initiatives, nowhere were the gaps in security more startling than in the importation of cargo packaged in shipping containers. Shipping containers travel the seas and enter ports with seeming anonymity and little verification of their contents.

Though a particular port “may accommodate anything from recreational watercraft, to barges, ferries, and ocean-going cargo and passenger ships,”¹ many ports along the southeastern United States tend to operate predominantly as cargo ports and are large contributors to the global supply chain. Given the robust container ports in the southeastern United States, including North and South Carolina, changes in

1. American Association of Port Authorities, U.S. Public Port Facts, <http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032&navItemNumber=1034> (last visited Sept. 11, 2007).

container security measures are of great concern in these communities.

This article describes the currently perceived threats of terrorist attacks on port facilities,² focuses on several container-specific legal developments aimed at protecting United States ports from terrorist threats, and briefly contemplates the role of technology and the government's current layered approach to port security and protection of the international supply chain involving container shipments. Consideration is given to the ultimate goal—protecting port facilities and communities from violent terrorist attacks without creating economically dangerous inefficiency or unnecessary costs.

In discussing these issues, this article concentrates on efforts to secure maritime shipping containers entering United States ports from other nations. Specifically, this article focuses on a handful of key legislative and executive initiatives undertaken or implemented by the U.S. Custom and Border Patrol (CBP) and the Department of Energy (DOE).

Also included by way of factual background is a brief explanation of the United States port system and its place in international trade. To explain the relevance of efforts to secure shipping containers, some statistics about the current size, type of business, and likely future expansion of ports in North and South Carolina are provided. Each port, such as those in the Carolinas, handling large volumes of imports arriving via shipping containers, may provide a means of entry for the individuals or weapons to be used in the next terrorist attack.

I. SHIPPING CONTAINERS: THE MODERN DAY TROJAN HORSE

The security weaknesses surrounding shipping containers are not typically the first concern when considering overall port security. For example, when news first broke that Dubai Ports World—through its purchase of Peninsular and Oriental Steam Navigation Company, a company already leasing marine terminals around the world, including five United States ports—may take over operation of several marine terminals in this country,³ many appeared to assume security would

2. This article focuses specifically on issues surrounding the security of ports handling container shipments. This article does not seek to address in any detail the entirety of all terrorist threats or related security issues for all maritime activities. Potential terrorist threats to maritime activities include everything from attacks on the high seas to immigration.

3. Though the Dubai Ports debate is not the subject of this article, it is noteworthy that “most United States container terminals are managed by foreign companies.” JOHN FRITTELLI & JENNIFER E. LAKE, CONG. RESEARCH SERV., TERMINAL OPERATORS AND

be newly threatened by the involvement of foreign entities in port operations.⁴

As will become apparent, not only are foreign entities already heavily invested in United States port operations, but the cooperation of private and governmental interests in other countries is crucial to securing, among other things, container shipments into United States ports. Rather than foreign investment, the real security issue surrounding shipping containers is the anonymity of those involved with the shipment and of the cargo actually contained inside. Regardless of any opposition to marine terminal or other port facility operations, “ports are vulnerable to the entry of terrorists or illicit weapons because of the large number of containers that enter U.S. territory, regardless of who manages them.”⁵

Shipping containers are large, standardized containers in which goods are packed and then transported. The most common sizes are twenty or forty foot containers. Each container can hold goods from many different manufacturers. Once loaded and transported to ports, they are loaded on vessels, with a single vessel able to accommodate 6,000 to 7,000 standard containers.⁶ “Containers can hold just about anything: frozen beef going from Buenos Aires to Rotterdam, LCD monitors heading from Hong Kong to Los Angeles, and even subway cars being exported from Hamburg to Shanghai.”⁷

The invention of shipping containers is relatively young, dating to the mid-1950s.⁸ Despite their youth, however, these containers have globalized the world economy⁹ and their use is continuously growing.¹⁰ Indeed, “[t]he container market is growing nearly three times as

THEIR ROLE IN U.S. PORT AND MARITIME SECURITY 4 (2006), <http://www.ni2ciel.org/Reference/Download.pm/5601/Document.PDF>.

4. *Dubai Company Gives Up on Port Deal: Move Comes as GOP Leaders Warn Bush That Congress Will Block Takeover*, CBS NEWS, Mar. 9, 2006, <http://www.cbsnews.com/stories/2006/03/09/politics/main1385030.shtml>.

5. Bill Gertz, *Security Fear About Infiltration by Terrorists*, WASH. TIMES, Feb. 22, 2006, at A01.

6. Alexander Jung, *The Box That Makes the World Go Round*, SPEIGEL ONLINE, NOV. 25, 2005, <http://www.spiegel.de/international/spiegel/0,1518,386799,00.html>.

7. *Id.* The troubling aspect of the “anything” that may be packaged in a shipping container is the potential that the cargo may include supplies for terrorist operations, weapons, or even the terrorists themselves.

8. *See id.*; *see also* MARC LEVINSON, *THE BOX: HOW THE SHIPPING CONTAINER MADE THE WORLD SMALLER AND THE WORLD ECONOMY BIGGER* (2006).

9. What is meant here by a globalized world economy or globalization is the increasingly integrated world economy in which goods and capital flow freely among nations.

10. *See Jung, supra* note 6.

fast as the world economy.”¹¹ But without the shipping container, globalization may not have been as easily achieved.

Globalization drives containerized cargo, and containers fuel globalization. Steel boxes have become the building blocks of the new global economy. Without this ingeniously simple, stackable and standardized receptacle, we would still be waiting for China’s economic miracle, and the American urge to spend, spend, spend would have been stifled in its infancy.¹²

The rise of shipping containers, though beneficial to world trade and globalization, also creates security concerns. These concerns stem from the limited scrutiny at ports of arriving cargo, the large volume of containerized cargo arriving at ports around the world, and the very fact that closed containers do not lend themselves to easy or economically efficient inspection.

In 2005, Senator Carl Levin of Michigan referred to ports as a modern day “Trojan horse.”¹³ Other government officials voiced similar concerns for the perceived holes in overall port security.¹⁴ Maritime experts had been warning of the “Trojan Horse” style threat of shipping containers as well.¹⁵ Indeed, many quickly concentrated on the unique risks posed by container shipments, shipping containers having also been characterized as a potential “poor man’s missile.”¹⁶

The use of containers in the global supply chain involves a complex network of manufacturers, exporters, importers, brokers, carriers and foreign customs and port officials. What ultimately arrives in a shipping container shipped to a United States port depends on the actions and information provided by these numerous entities and individuals. Everyone from manufacturers to land carriers to middlemen freight forwarders to customs brokers, terminal operators and port

11. *See id.*

12. *Id.*

13. *See Statement of Senator Carl Levin: Securing Global Supply Chain or Trojan Horse?*, STATES NEWS SERVICE, May 26, 2005, available in LEXIS, States News Service database.

14. *See, e.g.*, Interview with Senator Norm Coleman, Fox News Network (Mar. 28, 2006); Greg Krikorian, *Improved Security at Ports Urged*, L.A. TIMES, Feb. 24, 2005, at 4 (quoting Senator Dianne Feinstein).

15. *See, e.g.*, Patrick Yoest, *2006 Legislative Summary: Port Security Enhancements*, CONG. QUARTERLY WEEKLY REP. (2006).

16. *See Hearing on Sec. of Ocean Shipping Containers Before the Comm. on S. Homeland Sec. and Governmental Affairs Subcomm. on Permanent Investigations*, 109th Cong. (2005) [hereinafter Flynn Testimony 1] (testimony of Commander Stephen E. Flynn, U.S.C.G., retired, & Jeane J. Kirkpatrick, Senior Fellow for National Security Studies at the Council on Foreign Relations).

employees (including management, stevedores, and longshoremen) at every port entered by the carrying vessel play a role in securing the cargo and the locations to which it is sent.¹⁷ The many hands that access a single container create a number of significant container security issues.

Opportunities for security breaches occur primarily in the following stages of the shipping process: (1) the packing process at the foreign warehouse or factory; (2) the transport of the packed goods from that location to the foreign port at which the goods will be loaded; and (3) the preparation of the cargo manifest setting forth the contents and other information about the goods being shipped.¹⁸ Given these opportunities to tamper with the shipment process, container security efforts focus in large part on container inspection and documentation, container seals, and the secure storage of containers.

The many steps in the shipment of goods via shipping container from manufacturer to end consumer provide opportunities for tampering to petty criminals and terrorists alike. Unfortunately, the risks with which ports and customs officials remain most familiar are those associated with normal criminal activity, not terrorism.

Efforts that effectively address traditional criminal concerns, such as drug smuggling and human trafficking, may not aid in identifying containers posing a high risk of terrorist use. “[W]hat may have made sense for combating crime does not automatically translate to combating determined terrorists.”¹⁹ Indeed, at least three distinctions exist between basic criminal activity and the likely actions of terrorists:

17. A container shipped from a foreign manufacturer is likely to involve numerous private and governmental players. See, e.g., DEP’T OF HOMELAND SEC., STRATEGY TO ENHANCE INTERNATIONAL SUPPLY CHAIN SECURITY 39 (July 2007), <http://www.dhs.gov/xlibrary/assets/plcy-internationalsupplychainsecuritystrategy.pdf> (discussing the likely path of a fictitious container to include originally being “subject to the commerce and transportation laws and regulations of the originating nation as it is manufactured, containerized, and transported to a port,” then “mov[ing] into [the] jurisdiction of that nation’s customs organization[, moving] from Customs jurisdiction to that of the Nation’s maritime administration[, departing] the nation’s maritime jurisdiction and enter[ing] international waters, where it would be subject to multiple international agreements and where the vessel could conceivably be under the control of a second nation serving as the vessel’s Flag State[, moving] into the jurisdiction of the USCG[, arriving] at the port and transfer[ring] into the jurisdiction of CBP” and released first to the TSA and then ultimately for transport within the United States and subject to state and local authorities. Finally, upon release by CBP, the cargo becomes subject to State and local oversight).

18. FRITTELLI & LAKE, *supra* note 3, at 15.

19. *The Limitations of the Current U.S. Gov’t Efforts to Secure the Global Supply Chain Against Terrorist Smuggling a WMD and a Proposed Way Forward: Hearing on*

- (1) most security measures focus on identifying criminal patterns and behaviors in order to identify high risk shipments, whereas would-be terrorists are typically engaged in one-time operations;
- (2) rather than avoiding legitimate channels of trade to evade detection of ongoing criminal activity, terrorists have no reason not to use, and likely would prefer to use, legitimate companies and methods of shipment into the United States banking on such shipments being subjected to little or no inspection; and
- (3) traditional criminal use of legitimate companies and shipping avenues would result in unwanted attention and inspection of future smuggling shipments, whereas the use of such trusted shipments by terrorists furthers their goal of economic disruption.²⁰

Many post-9/11 port security efforts, particularly in their current forms, seek to deal with these differences between the traditional criminal and the terrorist.

Key efforts in this strategy operated by CBP include use of the Automated Targeting System (ATS),²¹ the 24-Hour Rule,²² the Customs-Trade Partnership Against Terrorism (C-TPAT),²³ and the Container Security Initiative (CSI).²⁴ The DOE also contributes to the security of container shipments. Two DOE programs that are intricately intertwined with these CBP initiatives include the Megaports

Neutralizing the Nuclear and Radiological Threat: Securing the Global Supply Chain Before the Senate Permanent Subcomm. on Investigations Comm. on Homeland Sec. and Governmental Affairs, 109th Cong. (2006) [hereinafter Flynn Testimony 2] (written testimony of Stephen E. Flynn, U.S.C.G., retired, & Jeane J. Kirkpatrick, Senior Fellow for National Security Studies at the Council on Foreign Relations), available at <http://www.cfr.org/publication/10277/>.

20. *Id.*

21. See SAFE Port Act of 2006 § 203, 6 U.S.C.A. § 943 (West 2007); see also Bureau of Customs and Border Protection, *Facts Concerning the Automated Targeting System*, Dec. 8, 2006, http://www.cbp.gov/xp/cgov/newsroom/highlights/cbp_responds/facts_automated_targeting_sys.xml.

22. See 19 C.F.R. § 4.7(b)(2) (2007).

23. See SAFE Port Act of 2006 §§ 211-23, 6 U.S.C.A. §§ 961-73 (West 2007); see also Bureau of Customs and Border Protection, C-TPAT Frequently Asked Questions, http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ctpat_faq.xml (last visited Dec. 5, 2007); BUREAU OF CUSTOMS AND BORDER PROTECTION, FACT SHEET, CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT) (2007), http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/port_security/ctpat.ctt/ctpat.pdf.

24. See SAFE Port Act of 2006 § 205, 6 U.S.C.A. § 945 (West 2007); see also Bureau of Customs and Border Protection, CSI In Brief, http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml (last visited Dec. 5, 2007) (providing a general overview of CSI).

program²⁵ and the very recently implemented Secure Freight Initiative.²⁶ Each of these programs is later discussed in more detail.²⁷ First, however, an understanding of the operations of United States ports is necessary.

Understanding the port system provides a paradigm in which to contemplate how these government programs provide improved security for the international supply chain. Moreover, some basic information on the volume of container cargo handled by ports in North and South Carolina helps stress the relevance of container security measures even for smaller, less urban areas than those often viewed as the most likely terrorist targets.

II. UNITED STATES PORTS: THE BACKBONE OF THE INTERNATIONAL SUPPLY CHAIN

The United States is served by more than 360 commercial ports that provide approximately 3,200 cargo and passenger handling facilities, according to the U.S. Coast Guard. Depending on the individual port facilities, they may accommodate anything from recreational watercraft, to barges, ferries, and ocean-going cargo and passenger ships. Governance of these ports in the United States is a function of various state and local public entities, such as port authorities, port navigation districts and municipal port departments. Currently, there are more than 160 cargo- and passenger-handling ports under the jurisdiction of 126 public seaport agencies located along the Atlantic, Pacific, Gulf and Great Lakes coasts, as well as in Alaska, Hawaii, Puerto Rico, Guam, and the U.S. Virgin Islands. Many of these seaport agencies are governed by an elected and/or appointed body, such as a port commission.²⁸

25. See NAT'L NUCLEAR SEC. ADMIN., MEGAPORTS INITIATIVE, http://www.nnsa.doe.gov/docs/megaports_initiative.pdf.

26. SAFE Port Act of 2006 §§ 224-25, 6 U.S.C.A §§ 981-981a (West 2007); see also Press Release, DHS and DOE Launch Secure Freight Initiative (Dec. 7, 2006), available at http://www.dhs.gov/xnews/releases/pr_1165520867989.shtm.

27. These initiatives, though central to the government's cargo security strategy, represent only a scratch on the surface of the Federal Government's cargo security plan. In addition to CBP and DOE, numerous other agencies are involved in security measures, including the U.S. Coast Guard. See, e.g., Regulation of Anchorage and Movement of Vessels During National Emergency Act, 50 U.S.C.A. § 191 (West Supp. 2007); Ports and Waterways Safety Act, 33 U.S.C. §§ 1221 *et seq.* (200 and Supp. 2004).

28. American Association of Port Authorities., U.S. Public Port Facts, <http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032&navItemNumber=1034> (last visited Sept. 11, 2007).

Some of these ports may not handle large quantities of cargo or may handle bulk cargo but not cargo carried in containers. What is clear is that the volume of those ports welcoming container shipments will continue to increase. Between 2001 and 2020, international container shipments are expected to double.²⁹ Though presumably good news for world trade, the increase in container shipments also mandates the need for efficient and effective methods of screening containers.

To consider competently any proposed method for undertaking to secure container shipments, an understanding must exist about the functioning of the particular port, the most likely risks of criminal activity faced by that port, and the resources available for combating those activities. A port that primarily handles cargo faces different issues than one typically used for passenger travel. Similarly, the volume of cargo or passengers will impact how the port operates, as well as what types of security measures are even feasible. In this regard, the current status of the ports in Charleston, South Carolina and Wilmington, North Carolina is instructive of the need for container security for shipments to these ports.

A. *Charleston*

The port of Charleston handles one of the highest volumes of shipping containers in the southeast and gulf coast regions.³⁰ Indeed, in 2006 it was the tenth busiest United States port in terms of container traffic when measured in Twenty-Foot Equivalent Units (TEUs).³¹ In 2005, ranked by cargo tons rather than TEUs, Charleston was recognized as the 33rd busiest port in overall trade and the 20th busiest port in cargo tons of imports.³²

29. *Id.*

30. See S.C. STATE PORTS AUTH., FACT SHEET 1 (2007), http://www.port-of-charleston.com/About_the_Port/statistics/FACT_SHEET_CY07.pdf.

31. See American Association of Port Authorities, World Port Ranking - 2005, <http://aapa.files.cms-plus.com/Statistics/WORLD%20PORT%20RANKINGS%202005.xls> (last visited Nov. 6, 2007). As defined by AAPA, a TEU is "a standard linear measurement used in quantifying container traffic flows. As examples, one twenty-foot long container equals one TEU while one forty-foot container equals two TEUs (i.e., 40'÷20'=2)." American Association of Port Authorities, Port Industry Statistics, <http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=900> (last visited Nov. 6, 2007).

32. See U.S. ARMY CORPS OF ENG'RS, WATERBORNE COMMERCE STATISTICS CTR., WATERBORNE COMMERCE OF THE UNITED STATES 5-4 (2005), <http://www.iwr.usace.army.mil/ndc/wesc/pdf/wcusnat05.pdf>.

The Charleston port annually welcomes more than 30 different ocean carrier lines from 150 nations.³³ It is this large volume of foreign goods entering the United States through this port that raises security concerns. The port in Wilmington, North Carolina, though smaller, faces similar issues as a container cargo port.

B. Wilmington

Despite its position in a state that is one of the top in manufacturing and distribution of goods, Wilmington neither handles nor is it equipped to handle the volume of cargo traffic currently passing through Charleston. As such, Wilmington's port receives less attention from federal agencies and others in terms of security measures. Nonetheless, Wilmington (along with other North Carolina ports) is growing.

Between 2005 and 2006, Wilmington saw a 19.4% increase in TEUs.³⁴ Although still well below the volume flowing through Charleston—177,634 TEUs as compared to Charleston's 1,968,474 TEUs³⁵—this increase indicates a likely expansion of Wilmington's role in international trade. Port officials and private businesses clearly expect continued growth. The Port of Wilmington is in the midst of a five-year, \$143 million, container terminal expansion.³⁶ Most recently, that expansion included the arrival of four new container cranes in operation since April 9, 2007.³⁷

Though both Charleston and Wilmington do welcome some non-container cargo, as well as occasional passenger vessels, it is the risks associated with the import of container shipments that should and likely do lie at the forefront of security concerns for these container ports. The potential threats to ports handling large volumes of container shipments are startling.

33. South Carolina State Ports Authority, Top Trade Routes, http://www.port-of-charleston.com/About_the_Port/statistics/traderoutes.asp (last visited Sept. 11, 2007).

34. See American Association of Port Authorities, U.S./Canada Container Traffic in TEUs (1980-2006), http://www.aapa-ports.org/files/Statistics/CONTAINER_TRAFFIC_CANADA_US.xls (last visited Nov. 6, 2007).

35. See *id.*

36. See North Carolina Ports, Port of Wilmington's Container Cranes Dedicated, <http://www.ncports.com/web/ncports.nsf/pages/070421+Cranes> (last visited Nov. 6, 2007).

37. *Id.*

III. TERRORIST THREATS

While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime and surface transportation. Initiatives to secure shipping containers have just begun.³⁸

Annually, more than nine million containers enter United States ports and most ships carrying these containers are foreign owned, foreign registered and operated by foreign crews.³⁹ Thus, any threat of terrorist use of shipping containers or container carrying vessels does not merely arise upon entry into a United States port. Rather, it is too late to combat the threat once the vessel on which terrorists, their supplies or weapons are loaded sail into domestic waters. It is one goal of port security to prevent terrorist entrance into United States waters altogether.

The way in which containers are used to pack and carry cargo complicates container security. A single container may contain cargo from many different companies and shippers. These containers are typically loaded somewhere other than the port (e.g., at company warehouses). Each cargo shipment may involve numerous persons and numerous stops from the actual exporter and importer to the various transportation providers that carry the cargo to and from the ports. Each time a container is transferred or opened a risk of tampering or the loading of dangerous cargo exists.

Moreover, given economic concerns, attacks targeting United States interests need not occur at or near any of the over three hundred domestic ports; such attacks could occur among ports of foreign nation trading partners.⁴⁰ Containers discharged at ports outside the United States, such as Canadian ports, may ultimately be transferred via truck or train into the United States. At all stages of shipment, security measures are needed and the cooperation of public and private parties in both the United States and abroad is vital. It is in every

38. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE US, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 391 (2004), <http://www.gpoaccess.gov/911/pdf/fullreport.pdf>.

39. See JOHN F. FRITTELLI, CONG. RESEARCH SERV., PORT AND MARITIME SECURITY: BACKGROUND AND ISSUES FOR CONGRESS (2005), <http://www.fas.org/sgp/crs/homesecc/RL31733.pdf>.

40. PAUL W. PARFOMAK & JOHN FRITTELLI, CONG. RESEARCH SERV., MARITIME SECURITY: POTENTIAL TERRORIST ATTACKS AND PROTECTION PRIORITIES 5 (2007), <http://www.fas.org/sgp/crs/homesecc/RL33787.pdf>.

trading country's interest to participate in efforts to secure these shipments.⁴¹

Analysis of the ways in which terrorists may use container shipments is not based on mere hypothesis. On October 18, 2001, a stowaway was discovered within a shipping container ultimately bound for Canada.⁴² The stowaway was discovered while the container was at the Italian port of Gioia Tauro.⁴³ This "stowaway," Rizik Amid Farid, was a suspected Al Qaeda member and an Egyptian national.⁴⁴ He was traveling in a container that was outfitted with a bed, a heater, toilet facilities and water.⁴⁵ More disturbing were the items he carried with him; a Canadian passport, phones, a computer, airport security passes and an airline mechanic's certificate that would enable him entry into sensitive areas at airports in New York, Chicago and Los Angeles.⁴⁶ Soon after his arraignment and release on bond, Farid disappeared.⁴⁷

Moreover, entire vessels are actually controlled by Al Qaeda. This terrorist organization may use those vessels for legitimate trade to raise funds or to carry out further terrorist activities.⁴⁸ The ease with which

41. DEP'T OF HOMELAND SEC. AND DEP'T OF DEFENSE, THE NATIONAL STRATEGY FOR MARITIME SECURITY 2 (2005), http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf ("Nations have a common interest in achieving two complementary objectives: to facilitate the vibrant maritime commerce that underpins economic security, and to protect against ocean-related terrorist, hostile, criminal, and dangerous acts. Since all nations benefit from this collective security, all nations must share in the responsibility for maintaining maritime security by countering the threats in this domain.").

42. MARITIME TRANSPORT COMMITTEE, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, SECURITY IN MARITIME TRANSPORT: RISK FACTORS AND ECONOMIC IMPACT 7-8 (2003), <http://www.oecd.org/dataoecd/63/13/4375896.pdf> [hereinafter OECD Report].

43. *Id.*

44. Tony Bartelme, *Coast Guard Warns of Stowaway Terrorists*, THE POST AND COURIER, (Charleston, S.C.), Oct. 31, 2001, at 13A; see also Tom Godfrey, *Stowaway Terror Suspect; Had Canuck Passport, Security Passes for Airports*, THE TORONTO SUN, Oct. 26, 2001, at 2.

45. OECD Report, *supra* note 42, at 7.

46. *Id.*

47. *Id.* at 7-8.

48. See William K. Rashbaum & Benjamin Weiser, *A Tramp Freighter's Money Trail to bin Laden*, N.Y. TIMES, Dec. 27, 2001, available at <http://query.nytimes.com/gst/abstract.html?res=F30810FD0B550C748EDDAB0994D9404482/> (claiming Al Qaeda ownership or links to at least 20 vessels) and also available at (for non-subscribers) <http://news/pseka.net/index.php?module=article&is=135&PHPSESSID=46eca01da7d32a265f98daced99f2f2c00>; see also John Mintz, *15 Freighters Believed to be Linked to Al Qaeda*, WASH. POST, Dec. 31, 2002, at A1.

Farid clearly used a container for his own transport—only discovered when he attempted to widen ventilation holes with port employees nearby—is disturbing.⁴⁹ This successful concealment of container contents, along with potential Al Qaeda control of entire vessels able to carry thousands of shipping containers, is particularly troubling when the total volume of maritime container shipments in need of security screening is considered.

“More than 80 percent of the world’s trade travels by water and forges a global maritime link. About half the world’s trade by value, and 90 percent of the general cargo, are transported in containers.”⁵⁰ Large volumes of trade via container shipments are processed through ports. Those ports also provide economic benefits to the surrounding communities.⁵¹ Thus, threats by terrorists may have several objectives, including human casualties, environmental damage or economic loss and disruption.⁵²

Despite terrorism recently becoming a primary port concern, containers are notoriously and continuously used for other criminal purposes. Shipping containers are used to ship illegal drugs, arms and munitions, undocumented workers, and even nuclear equipment and technology.⁵³

49. OECD Report, *supra* note 42, at 8.

50. DEP’T OF HOMELAND SEC. AND DEPT. OF DEFENSE, *supra* note 41, at 1-2. *See also* UNITED NATIONS CONFERENCE ON TRADE AND DEV. (UNCTAD), REVIEW OF MARITIME TRANSPORT (2002), http://www.unctad.org/en/docs/rmt2003_en.pdf.

51. International trade through the Port of Charleston, for example, provides 281,660 jobs (paying \$9.4 billion in wages), \$23 billion into the South Carolina economy, and \$2.5 billion in state and local taxes. *See* S.C. PORT AUTH. FACT SHEET, *supra* note 30.

52. Potential terrorist attacks include the following possible actions as identified by security experts:

- Use of cargo containers to smuggle terrorists, nuclear, chemical or biological weapons or components of those weapons;
- Use of cargo containers to ship other dangerous materials;
- Use of a large cargo ship as a collision weapon, much as aircraft were used on September 11, 2001, targeting bridges, refineries or other waterfront targets;
- Sinking a large cargo ship in a major shipping channel to block traffic to and from certain ports;
- Use of land surrounding ports to stage attacks on bridges, waterfront refineries, or port facilities themselves.

JOHN F. FRITTELLI, *supra* note 39, at 5.

53. OECD Report, *supra* note 42, at 8-9, 14. *See also* Port and Maritime Security Act, S. 1214, 107th Cong. (2001) (as reported by S. Comm. on Commerce, Science and Transp. 2002); S. REP. No. 107-64, at 5 (2001).

One of the most unsettling, suspected uses of shipping containers was by former-Pakistan nuclear program head, Abdul Qadeer Khan.⁵⁴ Khan, who admitted to selling nuclear technology to Iran, Libya and North Korea⁵⁵ is suspected of having used shipping containers to complete these sales, including a shipment inspected in August 2003 in the Mediterranean.⁵⁶ The shipment allegedly included the transport of elements of a future Libyan nuclear plant.⁵⁷

Moreover, terrorists may look to use legitimate, mislabeled cargo for their own heinous purposes. Based on the often erroneous identity of the cargo within a container – whether due to intentional deception or carelessness – numerous incidents of improperly handled hazardous materials exist. For example, in 1992, a storm damaged the vessel *Santa Clara I* in waters off the eastern coast of the United States.⁵⁸ Some containers aboard the vessel contained magnesium phosphide, which when mixed with air or water forms the highly reactive, flammable gases phosphene and diphosphane.⁵⁹ The containers in which these compounds were shipped did not identify the cargo as hazardous contents.⁶⁰ The danger posed by the spill of the compounds into the water in the port of Baltimore was not realized until the vessel reached its next port, Charleston, South Carolina.⁶¹

The situation on the *Santa Clara I* was not a terrorist act. The incident is, however, evidence of the ease of improperly manifesting shipping containers without detection. The fact that the *Santa Clara I*'s cargo was – though perhaps innocently – improperly identified without detection until the contents were spilled (and likely never would have been detected absent the spill caused by the storm damage) demonstrates that terrorists too may attempt to misidentify cargo contained in shipping containers. Terrorists may bank on this histori-

54. See Global Security, Weapons of Mass Destruction: A.Q. Khan, <http://www.globalsecurity.org/wmd/world/pakistan/khan.htm> (last visited on Aug. 29, 2007) [hereinafter Global Security]; Bernard-Henri Levy, *The Islamic Bomb: Abdul Qadeer Khan*, WALL STREET JOURNAL, Feb. 17, 2004, available at <http://www.opinionjournal.com/editorial/feature.html?id=110004702>.

55. *Id.*

56. Levy, *supra* note 54.

57. See Global Security, Weapons of Mass Destruction: A.Q. Khan, <http://www.globalsecurity.org/wmd/world/pakistan/khan.htm> (last visited on Aug. 29, 2007) [hereinafter Global Security]; Bernard-Henri Levy, *The Islamic Bomb: Abdul Qadeer Khan*, WALL STREET JOURNAL, Feb. 17, 2004, available at <http://www.opinionjournal.com/editorial/feature.html?id=110004702>.

58. OECD Report, *supra* note 42, at 8-9.

59. See *id.* at 9.

60. See *id.* at 8-9.

61. *Id.* at 9.

cally demonstrated possibility that the true identity of their cargo – whether itself legal or illegal absent any terrorist ties – may never be detected.

Container shipments are indisputably used for illicit purposes. To date, and to our knowledge, potential terrorists attempting to use the anonymity of container shipments to their advantage have all been detected – Farid – or are known to and presumably monitored by the United States – al Qaeda owned vessels. The government has not yet publicly identified any specific terrorist threats to container shipments or the ports through which such shipments pass, but serious gaps in container security required attention. “Like many parts of our society, we thus confront an unknown threat, but a known vulnerability.”⁶²

The only way wholly to ensure terrorists are unable to use containers to import weapons, other supplies or even would-be terrorists themselves is greater, indeed complete, physical inspection of incoming containers. Such inspections would need to be conducted prior to the carrying vessel’s entry into U.S. waters. Searches of all entering containers – or even inspection of any statistically significant number of containers – is extremely impractical. The impracticality of large scale inspections is clear when one considers that even now only about 5%⁶³ of containers entering United States ports are examined to identify their contents. Any large scale expansion of the number of containers examined – whether using non-intrusive imaging technology or involving an actual physical search – would be overly burdensome on global trade. Indeed, such security measures may themselves serve one of the potential terrorist goals by slowing maritime trade to an economically unacceptable level.⁶⁴

The goal in container security then must be to strike the proper balance between security and economic efficiency. Numerous steps have been taken to reach that goal, creating a layered approach aimed

62. *The SAFE Port Act: Hearing Before the H. Comm. on Homeland Sec.*, 109th Cong. 2 (2006) (testimony of Christopher Koch, President and CEO of the World Shipping Council), available at http://www.worldshipping.org/testimony_house_homeland_security_committee.pdf [hereinafter Koch Testimony].

63. See Susan E. Martinosi, David S. Ortiz & Henry H. Willis, *Evaluating the Viability of 100 Per Cent Container Inspection at America’s Ports*, in *THE ECONOMIC IMPACTS OF TERRORISM ATTACKS* 218, 221 (Harry W. Richardson, Peter Gordon, James E. Moore II eds., 2005), available at http://www.rand.org/pubs/reprints/2006/RAND_RP1220.pdf.

64. See Admiral James M. Loy & Captain Robert G. Ross, *Global Trade: America’s Achilles Heel*, DEFENSE HORIZONS, Feb. 2002, available at <http://www.ndu.edu/inss/DefHor/DH7/DH07.pdf> (describing any statistically significant random search of containers “economically intolerable”).

at detecting the true contents of the Trojan horse prior to its arrival in the United States.

IV. DEFENDING AGAINST THE TROJAN HORSE

To secure container shipments and the ports through which they pass, policy and lawmakers must be cognizant both of the likely effectiveness of any proposed security measure and the impact of that measure on economic efficiency. To guarantee the security of container ports completely would require shutting them down, stopping the use of United States ports for global trade. Such an option is clearly impractical and undoubtedly unacceptable. More practical are the recent legal and policy developments, which prudently seek to partner governments, ports authority organizations, and foreign entities as voluntary participants in a layered security scheme. The goal is both protection of the port communities and protection of the international supply chain.

Customs officials acted quickly after 9/11 to address concerns about the potential terrorist use of containers to carry out their missions. Congress also acted relatively quickly to answer at least some concerns about container port security and the protection of economic interests.⁶⁵ Unlike some other national security efforts, battling the threat posed by the smuggling of terrorists or their supplies in shipping containers does not face the same constitutional restraints.

Border searches, which include the search of shipping containers seeking importation into the United States, are not subject to the warrant provisions of the Fourth Amendment to the Constitution.⁶⁶

65. Many cargo security initiatives are related to security directives found in the United Nations adopted International Ship and Port Security Code (ISPS Code). IMO Doc. SOLAS/CONF.5/34, annex 1 (Dec. 12, 2002) (containing Resolution 2 of the December 2002 conference, which contains in its annex the ISPS Code), *available at* http://www.imo.org/Safety/mainframe.asp?topic_id=583&doc_id=2689#resos (implemented by International Convention for the Safety of Life at Sea, Nov. 1, 1974, 32 U.S.T. 47, 1184 U.N.T.S. 276). The MTSA essentially codified the requirements of the ISPS Code. Moreover, a number of post-9/11 enactments that include provisions for cargo security, including more specifically container shipment security, are not addressed in this article. Those provisions include sections of the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002) (codified at 6 U.S.C. §§ 101 et seq. (Supp. IV 2004)); Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131-34 (Supp. IV 2004); Aviation and Transportation Security Act of 2001, Pub. L. No. 107-71, 115 Stat. 597 (2001).

66. *See* United States v. Ramsey, 431 U.S. 606, 617 (1977); *see also* United States v. Oriakhi, 57 F.3d 1290 (4th Cir. 1995) (deciding that even shipping containers leaving the United States may be subject to a warrantless search at the border).

The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, [the Supreme Court has] stated that "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."⁶⁷

Given that a warrant need not be obtained prior to screening or searching packed containers crossing United States borders, the government properly looked at ways to better and more thoroughly screen – and, if necessary, search – shipping containers bound for the United States as a means of reducing the risk of terrorist threats.

One of the first post-9/11 enactments addressing port security, the Maritime Transportation Safety Act of 2002 (the "MTSA"),⁶⁸ and the most recent port security legislation, the Security and Accountability for Every Port Act of 2006 (the "SAFE Port Act"),⁶⁹ codified many of CBP's post-9/11 efforts to secure container shipments and provided minimum standards for participation in existing CBP programs.⁷⁰ These programs represent a necessary shift from traditional criminal analysis of container risks to recognition of the unique characteristics of terrorist operations by providing a layered approach to port security. Moreover, these programs require a deviation from the pre-9/11 "us-versus-them" mentality between customs authorities and importers and exporters. Cooperation is necessary for the success of any counterterrorism strategy; no less so for the success of efforts to secure the integrity of container shipments. Security begins with information.

67. *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004) (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).

68. Maritime Transportation Safety Act of 2002, Pub. L. No. 107-295, 116 Stat. 2068 (codified at 46 U.S.C. §§ 70101 et. seq. (Supp. IV 2004)).

69. SAFE Port Act, Pub. L. No. 109-347, 120 Stat. 1884 (2006) (codified primarily in Title 6 of the United States Code).

70. Port security laws and programs, even when limited to container security, include many more government programs than those discussed here. Due to the breadth of information available about shipping container security efforts, this article attempts to select only those efforts most crucial the government's overall strategy to secure shipping containers.

A. *Automated Targeting System (ATS)*

CBP relies heavily upon the ATS.⁷¹

The Automated Targeting System, which is used by the National Targeting Center^[72] and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and “red flags,” and determine which passengers and cargo are “high risk,” and should be scrutinized at the port of entry, or in some cases, overseas.

ATS is a flexible, constantly evolving system that integrates enforcement and commercial databases. ATS analyzes electronic data related to individual shipments prior to arrival and ranks them in order of risk based on the application of algorithms and rules. The scores are divided into thresholds associated with further action by CBP, such as document review and inspection.⁷³

The ATS is not limited to analysis of incoming container shipments, though that is the aspect of the system discussed here.

ATS consists of six modules that provide selectivity and targeting capability to support CBP inspection and enforcement activities.

- ATS-Inbound - inbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Outbound - outbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Passenger (ATS-P) - travelers and conveyances (air, ship, and rail)
- ATS-Land (ATS-L) - private vehicles arriving by land

71. SAFE Port Act, 6 U.S.C.A. § 943 (West 2007).

72. The National Targeting Center is staffed with expert Targeters and Analysts, as well as field officers. This staff is comprised primarily of “CBP Officers and Analysts, representing Immigration, Customs and Agriculture expertise, as well as U.S. Border Patrol Officers and CBP Intelligence Analysts.” It consolidates and analyzes information across agencies to support counterterrorism efforts. See Bureau of Customs and Border Protection, Fact Sheet: U.S. Customs and Border Protection’s National Targeting Center (Sept. 7, 2004), available at http://www.dhs.gov/xnews/releases/press_release_0506.shtm.

73. *Efforts to Detect and Interdict Radiological or Nuclear Material: Hearing on Neutralizing the Nuclear and Radiological Threat: Securing the Global Supply Chain Before the Senate Permanent Subcommittee on Investigations Comm. on Homeland Security and Governmental Affairs*, 109th Cong. 3 (2006) (statement of Jayson P. Ahern, Asst. Commissioner, Office of Field Operations, U.S. Customs and Border Protection), available at http://hsgac.senate.gov/_files/STMTAhernCBP.pdf [hereinafter Ahern Statement].

- ATS - International (ATS-I) - cargo targeting for CBP's collaboration with foreign customs authorities
- ATS-Trend Analysis and Analytical Selectivity Program, (ATS-TAP) (analytical module)⁷⁴

In order to analyze the risk posed by a particular container's cargo, ATS-Inbound "[c]ollects information about importers, cargo, and conveyances used to facilitate the importation of cargo into the United States."⁷⁵ This information includes personal information about all individuals associated with the shipment, including brokers, carriers, shippers, buyers, sellers, and even the ship's crew.⁷⁶ Similarly, the ATS-I permits access, pursuant to agreements with other countries, to information collected by foreign customs authorities and, in exchange, permits those authorities restricted access to information collected by ATS-Inbound.⁷⁷

Despite privacy concerns not directly related to shipping containers⁷⁸ and concerns about the effectiveness of the ATS, proponents can properly point to the benefit obtained by removing hasty, arbitrary, and on-the-spot decision making of customs officials. The ATS removes much of the decision making from the customs official on the scene at a particular port. The system incorporates more factors than those available to such officials and uses computer scoring that represents the input of numerous experienced agents and information from a variety of sources. Unfortunately, the system still faces quality assurance challenges.

As of early 2007, CBP was still in the process of implementing several quality controls, including the following: "(1) performance

74. DEP'T OF HOMELAND SEC. PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM 3 (2006), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf [hereinafter PIA]. Container security for purposes of preventing terrorist attacks in U.S. ports focuses on ATS-Inbound and ATS-I. For that reason, the privacy issues surrounding much public debate about ATS, which focus in large part on the ATS-P module, are not discussed.

75. *Id.* at 5.

76. *Id.*

77. *Id.* at 6.

78. Current privacy concerns focus upon the information obtained about travelers and not about cargo. In other words, the privacy concerns stem from concerns about what information is being obtained and retained by government agencies regarding individuals traveling to and from the United States. Though ATS also gathers and analyzes personal data about individuals in the cargo context – such as information about the actual importers and exporters and ships' crew members – critics have not been as vocal about any privacy concerns surrounding these activities. Since this article focuses on the cargo portion of port security, privacy concerns are not addressed.

metrics^[79] to measure the effectiveness of ATS, (2) a comparison of the results of randomly conducted inspections with the results of its ATS inspections, and (3) a simulation and testing environment.”⁸⁰ One of the challenges facing CBP in its attempts to evaluate the effectiveness of ATS is the inability to halt screening activities in order to input internal controls.⁸¹ Perhaps the additional time provided by the 24-Hour Rule between the government’s receipt of manifest information about a shipment and the actual loading of the container aboard a vessel bound for the United States will assist in easing some of the challenge of implementing effective internal controls with ATS.

B. 24-Hour Rule

Information provided pursuant to the 24-Hour Rule represents some of the data analyzed by the Automated Targeting System (ATS). The 24-hour manifest rule applies to all ports - CSI and non-CSI ports⁸² - from which goods will be shipped to or through the United States.⁸³ Current regulations provide that “Customs and Border Protection (CBP) must receive from the incoming carrier, for any vessel covered under paragraph (a) of this section, the CBP-approved electronic equivalent of the vessel’s Cargo Declaration (Customs Form 1302), 24 hours before the cargo is laden aboard the vessel at the foreign port (see § 4.30(n)(1)).”⁸⁴

Current Form 1302 requires the following information: vessel name, nationality of the ship, IMO number,⁸⁵ the voyage number, name of the ship’s Master, the last foreign port visited by the vessel

79. ATS is described as “a complex mathematical model that uses weighted rules that assign a risk score to each arriving shipment based on manifest information.” *Maritime Security: Observations on Selected Aspects of the SAFE Port Act: Hearing Before the H. Subcomm. On Border, Maritime, and Global Counterterrorism. Comm. on Homeland Security* (2007), 110th Cong. 23 (statement of Stephen L. Caldwell, Director Homeland Security and Justice, United States Government Accountability Office), available at <http://hsc.house.gov/SiteDocuments/20070427081200-92787.pdf> [hereinafter Caldwell Statement].

80. *Id.* at 24.

81. *Id.*

82. The 24-hour rule also applies to all shipments regardless whether those involved in a particular shipment are members of C-TPAT.

83. See 19 C.F.R. § 4.7 (2007); see also Trade Act of 2002 § 343, 19 U.S.C. § §§ 3803-3805 and 68 Fed. Reg. 68140 (Dec. 5, 2003) (to be codified at 19 C.F.R. Parts 4, 103, 113, 122, 123, 178, 197).

84. 19 C.F.R. § 4.7(b)(2) (2007).

85. The IMO number is a ship identification scheme that became mandatory for all vessels in 1996. See Int’l Mar. Org., IMO ship identification number scheme, at http://www.imo.org/TCD/mainframe.asp?topic_id=388.

prior to entry into the United States, the port of discharge of the cargo, the date and time of departure from the port of loading, the name and address of shippers and consignees, the bill of lading number, Marks and Numbers, container numbers, seal numbers, the number and kinds of packages, a description of the goods carried and identification of any hazardous materials, gross weight or measurement of the cargo, the first port or place where the carrier takes possession of the cargo and the foreign port where the cargo is laden on board the vessel.⁸⁶ Additional manifest information is required to be maintained by the master onboard the vessel but need not be provided to any government agency 24-hours prior to loading.⁸⁷

The 24-Hour Rule applies to all cargo carried in containers but not to bulk cargo.⁸⁸ Instead, carriers of bulk cargo must provide cargo manifests to customs officials 24-hours *prior to arrival* at a United States port.⁸⁹ The required cargo manifest 24-hours *prior to loading* currently applies only to container cargo carried aboard “every vessel arriving in the United States and required to make entry.”⁹⁰ The distinction is obvious - shipping containers conceal cargo much more effectively than bulk shipments, which are more easily and readily examined and identified.

Some commentators, including those representing the concerns of those in the shipping industry, urged adoption of requirements that more information be provided to CBP prior to the loading of a vessel. Specifically, the World Shipping Council urged Congress during debate on the SAFE Port Act to require better cargo descriptions, identification of the party selling goods to an importer and the party purchasing those goods, the actual point of origin of the goods, the country of export, the ultimate consignee of the goods, the exporter representative and broker, and the origin of the container shipment.⁹¹ Though this information is generally required to be provided in the actual ship's manifest kept onboard, much of it remains unavailable to CBP prior to loading of the vessel. Given that currently government agencies do not have all information relevant to a particular container shipment and that they must rely on the accuracy of the information provided, cooperation with the private companies actually involved

86. See Dep't of Homeland Sec., Bureau of Customs and Border Protection, Form 1302, Form Approved OMB No. 1651-0001; Exp. 12/31/2008

87. See 19 C.F.R. § 4.7(a) (2007).

88. *Id.*

89. 19 C.F.R. § 4.7(b)(4) (2007).

90. 19 C.F.R. § 4.7(a) (2007).

91. See Koch Testimony, *supra* note 61.

with the shipments provides an additional layer of defense in the area of container shipments.

C. *Customs-Trade Partnership Against Terrorism (C-TPAT)*

C-TPAT is the prime example of coordination between private entities and government customs officials.

C-TPAT is a successful voluntary government-business initiative to build cooperative relationships that strengthen and improve overall international supply chain and United States border security. C-TPAT recognizes that CBP can provide the highest level of cargo security only through close cooperation with the ultimate owners of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers.⁹²

C-TPAT does not duplicate the requirements placed on those involved in container shipments by the ISPS Code and other national and international authorities. Instead, “C-TPAT seeks to build upon the ISPS and MTSA foundation and require additional security measures and practices which enhance the overall security throughout the international supply chain.”⁹³ It achieves this greater security through voluntary partnership with those involved in the various stages of container shipments. By meeting specified minimum security criteria “[i]mporters, customs brokers, forwarders, air, sea, land carriers, contract logistics providers, and other entities in the international supply chain and intermodal transportation system” may apply for and become participants in C-TPAT.⁹⁴

To become a C-TPAT participant, an application and approval by CBP is required.⁹⁵ CBP’s application review requires the applicant to provide information about its security plan and prior shipping experience, including the applicant’s demonstration of “a history of moving cargo in the international supply chain.”⁹⁶ CBP further assesses the applicant’s supply chain using established criteria.⁹⁷ That supply chain assessment includes a review of the applicant’s “(A) business

92. DEP’T OF HOMELAND SECURITY, STRATEGY TO ENHANCE INTERNATIONAL SUPPLY CHAIN SECURITY (July 2007), at 66, *available at* <http://www.dhs.gov/xlibrary/assets/policy-internationalsupplychainsecuritystrategy.pdf>.

93. *See* BUREAU OF CUSTOMS AND BORDER PROTECTION, C-TPAT SECURITY CRITERIA, SEA CARRIERS (Mar. 1, 2006), *available at* http://www.cbp.gov/xp/cgov/newsroom/full_text_articles/trade_prog_initiatives/adv_data_elements.xml (last visited on Aug. 8, 2007).

94. SAFE Port Act § 212, 6 U.S.C. § 962 (2007).

95. SAFE Port Act § 212, 6 U.S.C. § 962 (2007).

96. SAFE Port Act § 213(1), 6 U.S.C. § 963(1) (2007).

97. SAFE Port Act § 213(2), 6 U.S.C. § 963(2) (2007).

partner requirements; (B) container security; (C) physical security and access controls; (D) personnel security; (E) procedural security; (F) security training and threat awareness; and (G) information technology security.”⁹⁸

Through C-TPAT, CBP establishes voluntary best security practices for all parts of the supply chain, making it more difficult for a terrorist or terrorist sympathizer to introduce a weapon into a container being sent by a legitimate party to the United States. C-TPAT covers a wide variety of security practices, from fences and lighting to requiring that member companies conduct background checks on their employees, maintain current employee lists, and require that employees display proper identification.

C-TPAT’s criteria also address physical access controls, facility security, information technology security, container security, security awareness and training, personnel screening, and important business partner requirements. These business partner requirements encourage C-TPAT members to conduct business with other C-TPAT members who have committed to the same enhanced security requirements established by the C-TPAT program.⁹⁹

Applicants voluntarily seek to participate in C-TPAT in exchange for benefits provided by CBP. These benefits often take the form of decreased cargo examination and more expeditious access of the C-TPAT participant’s shipments into United States ports and ultimately into the United States economy.¹⁰⁰ The SAFE Port Act established three tiers for C-TPAT benefits. Those participants qualifying under the higher tiers, who have met more stringent security standards, are provided greater benefits and more efficient entry of cargo into the United States.¹⁰¹

The benefits provided to each tier of C-TPAT participants is determined by the Commissioner of the CBP.¹⁰² Those benefits may include lower scores in the Automated Targeting System (ATS), reduced cargo examinations, and priority searches to speed up the customs process for C-TPAT participants’ cargo shipments.¹⁰³

C-TPAT participants qualifying for higher tiers may be afforded larger reductions in ATS scores. For example, Tier 1 participants may

98. *Id.*

99. Ahern Statement, *supra* note 72.

100. SAFE Port Act §§ 214(a), 215(b), 216(c), 6 U.S.C. §§ 964(a), 965(b), and 966(c) (2007).

101. *See* SAFE Port Act §§ 214-216, 6 U.S.C. §§ 964-966 (2007).

102. *See* SAFE Port Act §§ 214-216, 6 U.S.C. §§ 964-966 (2007).

103. *See* SAFE Port Act §§ 214(a), 215(b), 216(c), 6 U.S.C. §§ 964(a), 965(b), 966(c) (2007).

receive ATS score reductions up to twenty percent (20%) of the high-risk threshold set by the Secretary of the Department of Homeland Security.¹⁰⁴ Tier 2 and 3 participants may receive even larger ATS score reductions.¹⁰⁵ Moreover, Tier 2 and 3 participants may be afforded priority searches of cargo, a benefit not provided to C-TPAT participants qualifying only for Tier 1 status.¹⁰⁶

Of the three tiers of C-TPAT participant requirements, all sea carrier participants must meet minimum standards for container security. The following are the standards established and published by CBP in March 2006:

Container Security

For all containers in the sea carrier's custody, container integrity must be maintained to protect against the introduction of unauthorized material and/or persons. Sea carriers must have procedures in place to maintain the integrity of the shipping containers while in their custody. A high security seal must be affixed to all loaded containers bound for the U.S. All seals used or distributed by the sea carrier must meet or exceed the current PAS ISO 17712 standards for high security seals [footnote omitted].

Sea carriers and/or their marine terminal operators must have processes in place to comply with seal verification rules and seal anomaly reporting requirements once promulgated and mandated by the U.S. government.

- **Container Inspection**

The requirement to inspect all containers prior to stuffing (to include the reliability of the locking mechanisms of the doors) is placed upon the importers through the C-TPAT Minimum Security Criteria for Importers dated March 25, 2005. Sea carriers must visually inspect all U.S.-bound empty containers, to include the interior of the container, at the foreign port of lading.

- **Container Seals**

Written procedures must stipulate how seals in the sea carrier's possession are to be controlled. Procedures should also exist for recognizing and reporting compromised seals and/or containers to US Customs and Border Protection or the appropriate foreign authority consistent with the seal anomaly reporting requirements once promulgated and mandated by the U.S. government.

104. SAFE Port Act § 214(a), 6 U.S.C. § 964(a) (2007).

105. SAFE Port Act §§ 215(b), 216(c), 6 U.S.C. §§ 965(b), 966(c) (2007).

106. SAFE Port Act §§ 214-216, 6 U.S.C. §§ 964-966 (2007).

- **Container Storage**

The sea carrier must store containers in their custody in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting detected, unauthorized entry into containers or container storage areas to appropriate local law enforcement officials.¹⁰⁷

As is apparent from these general security standards, in the realm of container shipments, inspection, sealing and storing are the core concerns.

Regardless of these generalized standards, critics of C-TPAT were quick to characterize the program's initial system as a "trust, but don't verify system."¹⁰⁸ When first initiated CBP aspired to validate the security of all C-TPAT participants within the first three (3) years of participation in the program.¹⁰⁹ The overwhelming number of C-TPAT applications and the quick growth of the program, however, created a backlog that prevented achieving this goal.¹¹⁰ As a result, CBP was forced to develop a method to select participants for validation based on risk factors "such as the company having foreign supply chain operations in a known terrorist area or involving multiple foreign suppliers."¹¹¹ Even those validations performed were criticized as not being sufficiently rigorous to confirm minimum security requirements were met.¹¹²

With passage of the SAFE Port Act, at least some of these concerns are addressed. CBP was directed to develop a pilot program using third party entities to conduct validations of C-TPAT participants.¹¹³ Relying solely on government resources, attempts at any validation process amounted to a sort of "spot-check" and even CBP's attempts at a minimal validation procedure were not fully implemented due to a lack of sufficient CBP staff.¹¹⁴ The use of third parties may provide the additional resources needed for validation of all C-TPAT participants.

107. See BUREAU OF CUSTOMS AND BORDER PROTECTION, C-TPAT SECURITY CRITERIA, SEA CARRIERS (Mar. 1, 2006), available at http://www.cbp.gov/xp/cgov/newsroom/full_text_articles/trade_prog_initiatives/adv_data_elements.xml (last visited on Aug. 8, 2007).

108. See Flynn Testimony 1, *supra* note 16.

109. See Caldwell Statement, *supra* note 78, at 30.

110. See *id.*

111. See *id.*

112. See *id.*

113. SAFE Port Act § 218, 6 U.S.C. § 968 (2007).

114. See Flynn Testimony 1, *supra* note 16.

By March 2006, CBP completed validations on only twenty-seven percent (27%) of the certified C-TPAT members.¹¹⁵ Though progress was made toward more validations prior to passage of the SAFE Port Act, the introduction of a pilot program of third party validating entities could likely, if it has not already,¹¹⁶ increase those numbers, despite the CBP's reluctance to use third party entities.¹¹⁷

The use of third parties for validation, along with the additional resources allocated to CBP's efforts,¹¹⁸ may also assist in meeting the clear timetables that were established for when each participant must undergo validation and when participants must undergo revalidation.¹¹⁹ Every C-TPAT participant must undergo validation of its security procedures within a year of being granted entry into the program and each participant must undergo revalidation at least once every four (4) years.¹²⁰

Despite continuing attempts to improve perceived weaknesses in C-TPAT, the growing number of participants is impressive. In March 2006, approximately 5,800 businesses were approved C-TPAT participants with over 10,000 businesses having applied for approval.¹²¹

Even with more thorough validation procedures, however, C-TPAT alone does not address all container shipment concerns. CSI, for example, works in conjunction with C-TPAT to address additional concerns of container screening.

D. Container Security Initiative (CSI)

Where C-TPAT seeks to identify all those involved in the shipping process to identify which containers may be subject to less scrutiny, the Container Security Initiative (CSI) focuses on CBP's own evalua-

115. Ahern Statement, *supra* note 72.

116. In its preliminary strategy report, STRATEGY TO ENHANCE INTERNATIONAL SUPPLY CHAIN SECURITY (July 2007) [hereinafter DHS Preliminary Report], the Department of Homeland Security stated that by the "end of January 2007, there were 6,375 certified members enrolled in C-TPAT and over 3,900 validations had been completed (61 percent)." DHS Preliminary Report at 66; *see also* Caldwell Statement, *supra* note 78, at 30. (stating that of the 6,375 companies certified by CBP as C-TPAT participants, validation was complete on 3,950 of them or 61.9 percent). The Report went on to state that "CBP will continue to use the validation approaches and strategies implemented throughout 2006 to reach 100 percent validations of all certified members due for validation or revalidation by the end of 2007." DHS Preliminary Report at 66.

117. *See* Flynn Testimony 2, *supra* note 19.

118. SAFE Port Act §§ 222, 223, 6 U.S.C. §§ 972, 973 (2007).

119. SAFE Port Act §§ 214-216, 219, 6 U.S.C. §§ 964-966, 969 (2007).

120. SAFE Port Act §§ 215(a), 219, 6 U.S.C. §§ 965, 969 (2007).

121. *See* Ahern Statement, *supra* note 72.

tion and examination of containers in foreign ports prior to their being laden on vessels bound for the United States. Once the potential for terrorist attacks on ports was identified, it was immediately apparent that efforts that could only identify weapons and other hazardous shipments once they arrived in United States ports did little to alleviate the risks to those ports, the supply chains they embody and the surrounding communities. CSI takes security efforts overseas and relies upon the cooperation of foreign ports and governments.

Although all containers are subject to “screening”¹²² to determine if further examination is necessary, in 2005 only five percent (5%) of all containers entering U.S. ports – those containers identified as high risk – were actually examined by CBP officials.¹²³ Of those examined containers, the examination actually conducted may occur at the foreign port of loading under CSI or upon arrival in the United States.¹²⁴ The examination could include radiation screening, non-intrusive x-ray inspection, or physical examination.¹²⁵

Though later CSI was codified,¹²⁶ it began as a U.S. Customs (now CBP) initiative. CSI was announced in January 2002,¹²⁷ just months after September 11. It is based on four key elements: “(1) using intelligence and automated information to identify and target high-risk containers; (2) pre-screening those containers identified as high-risk, at the port of departure, before they arrive at U.S. ports; (3) using detection technology to quickly pre-screen high-risk containers; and (4) using smarter, tamper-evidence containers.”¹²⁸ Despite recent codification of this initiative, these four basic goals of CSI remain the same.

122. “Screening’ is defined as a visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine the presence of misdeclared, restricted, or prohibited items and to assess the level of threat posed by such cargo.” DHS Preliminary Report at 70.

123. See Ahern Statement, *supra* note 72.

124. See *id.*

125. See *id.*

126. SAFE Port Act § 205, 6 U.S.C. § 945 (2007). The SAFE Port Act of 2006 codified the existing CSI and further required reports to Congress on the initiative’s effectiveness and the need for any improvements. The first such report is due September 30, 2007. *Id.*

127. See Press Release, CSI in Brief (Aug. 29, 2007), available at http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml.

128. Press Release, U.S. Customs and Border Protection, Secretary Ridge Announces Security Initiatives Phase II (June 12, 2003), available at http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/cbp_press_releases/062003/0612203_2.xml.

CSI seeks to achieve its goals through assessment of foreign ports, overseas inspections, and coordination with other agencies and the private sector to obtain the detection equipment necessary to support CSI. Foreign ports seeking to participate in CSI must first undergo assessment. That assessment requires review of many factors, including:

- (1) the level of risk for the potential compromise of containers by terrorists, or other threats as determined by the Secretary;
- (2) the volume of cargo being imported to the United States directly from, or being transshipped through, the foreign seaport;
- (3) the results of the Coast Guard assessments conducted pursuant to section 70108 of title 46, United States Code;
- (4) the commitment of the government of the country in which the foreign seaport is located to cooperating with the Department in sharing critical data and risk management information and to maintain programs to ensure employee integrity; and
- (5) the potential for validation of security practices at the foreign seaport by the Department.¹²⁹

Once the Secretary performs the assessment, the port may be designated under CSI. Once so designated, minimum standards are to be met by that port, including “standard operating procedures for the use of non-intrusive inspection and nuclear and radiological detection systems.”¹³⁰ To further implementation of these inspection standards, Congress directed coordination with other agencies, the private sector and the foreign governments in obtaining satisfactory detection equipment.¹³¹ The benefit of this assistance, and more specifically of designation as a CSI port, is that cargo loaded in such foreign ports may be deemed to present a lower risk than similar cargo loaded at a non-CSI designated port.¹³² As such, cargo from CSI ports - not just that shipped by C-TPAT participants - will be subject to less CBP scrutiny and will flow more rapidly through the international supply chain.

CSI is being implemented in three stages.¹³³ The first stage focused on the top twenty (20) megaports in order to garner their participation in the initiative.¹³⁴ When in 2003 nineteen of those twenty

129. SAFE Port Act of 2006 § 205(b), 6 U.S.C. § 945(b) (2007).

130. SAFE Port Act of 2006 § 205(e)(A), 6 U.S.C. § 945(e)(A) (2007).

131. See SAFE Port Act of 2006 § 205(g), 6 U.S.C. § 945(g) (2007).

132. See SAFE Port Act of 2006 § 205(j), 6 U.S.C. § 945(j) (2007).

133. See *id.*

134. Press Release, U.S. Customs and Border Protection, Secretary Ridge Announces Security Initiatives Phase II (June 12, 2003), available at http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/cbp_press_releases/062003/06122003_2.xml.

megaports implemented CSI, the second phase of the initiative was announced.¹³⁵ Though the third phase is not yet formally being implemented, additional ports continue to meet CSI standards and become CSI operational ports.¹³⁶

The ultimate success of CSI is unknown but a report to Congress on its effectiveness was due September 30, 2007.¹³⁷ Success will indeed depend in large part on the cooperation of foreign authorities in permitting CBP inspections prior to loading of containers identified as high risk. Moreover, effectiveness may be hindered by the failure of many foreign governments to obtain non-intrusive imaging, radiation detection, and other inspection equipment that meets satisfactory standards.¹³⁸ The DOE's Megaports Initiative seeks to assist in this regard by distributing radiation detection devices.

E. *Megaports Initiative*

The Megaports Initiative began in 2003 and seeks to enhance foreign countries' ability to screen cargo at their major seaports.¹³⁹ The initiative provides radiation detection equipment and also provides

135. *Id.*

136. As of July 27, 2007, the following ports were deemed by CBP as CSI operational ports: Montreal, Vancouver, and Halifax (Canada), Santos (Brazil), Buenos Aires (Argentina), Puerto Cortes (Honduras), Caucedo (Dominican Republic), Kingston (Jamaica), Freeport (The Bahamas), Rotterdam (The Netherlands), Bremerhaven and Hamburg (Germany), Antwerp and Zeebrugge (Belgium), Le Havre and Marseille (France), Gothenburg (Sweden), La Spezia, Genoa, Naples, Gioia Tauro, and Livorno (Italy), Felixstowe, Liverpool, Thamesport, Tilbury, and Southampton (United Kingdom), Piraeus (Greece), Algeciras, Barcelona, and Valencia (Spain), Lisbon (Portugal), Singapore, Yokohama, Tokyo, Nagoya and Kobe (Japan), Hong Kong, Pusan (South Korea), Port Klang and Tanjung Pelepas (Malaysia), Laem Chabang (Thailand), Dubai (United Arab Emirates), Shenzhen, Shanghai, Kaohsiun, Chi-Lung, Colombo (Sri Lanka), Port Salalah (Oman) and eDurban (South Africa). See BUREAU OF CUSTOMS AND BORDER PROTECTION, PORTS IN CSI (July 27, 2007), available at http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/ports_in_csi.xml.

137. SAFE Port Act of 2006 § 205(l), 6 U.S.C. § 945(l) (2007).

138. It is often the lack of resources in foreign ports that reduces effectiveness of programs such as the CSI and it is also this lack of resources that in many instances prevents the United States from establishing minimum technical requirements for the equipment purchased and used at these foreign locations. Some assistance is being provided to foreign ports by the United States. See later discussion on the Megaports Initiative, for example. This assistance, in addition to reaching some international consensus on minimum requirements for inspection technologies, will go a long way toward increasing cooperation of foreign ports authorities.

139. See, NAT'L NUCLEAR SEC. ADMIN., MEGAPORTS INITIATIVE, http://www.nnsa.doe.gov/docs/Megaports_Initiative.pdf.

training to foreign port officials. In exchange, the foreign government agrees to share information with DOE, specifically with the National Nuclear Security Administration housed in the DOE, about any detections or seizures of nuclear or radiological materials. “The Megaports Initiative is part of DOE’s Office of the Second Line of Defense, whose aim is to strengthen the overall capability to detect and deter illicit trafficking of nuclear and other radioactive materials across international borders.”¹⁴⁰ The initiative is implemented as follows: “(1) port prioritization; (2) government-to-government negotiations and port familiarization; (3) technical site surveys, site design, and training; (4) final design, construction, and equipment installation; (5) equipment calibration and testing; and (6) maintenance and sustainability.”¹⁴¹

Port prioritization involves the ranking of foreign ports to identify those ports that may be most attractive to persons or entities seeking to smuggle nuclear or radioactive materials and which, therefore, should be included in the program.¹⁴² Unfortunately, two years into the program many of the ports identified as presenting the greatest risk for nuclear smuggling were not yet agreeable to participate in the program.¹⁴³ Many hurdles blocked progress.

Political difficulties negotiating agreements with foreign countries and concerns about the additional resources (e.g., employees) participating countries would need to perform the required screening resulted in agreements with only two of the twenty countries in which the top priority ports were located.¹⁴⁴ Moreover, technical difficulties inherent in the actual screening equipment and procedures were less than certain to detect the presence of nuclear or radiological materials.¹⁴⁵

Nonetheless, DOE continues to negotiate agreements for additional participants in the Megaports Initiative. Despite less than glow-

140. GOV’T ACCOUNTABILITY OFFICE, REPORT TO CONGRESSIONAL REQUESTERS, PREVENTING NUCLEAR SMUGGLING: DOE HAS MADE LIMITED PROGRESS IN INSTALLING RADIATION DETECTION EQUIPMENT AT HIGHEST PRIORITY FOREIGN SEAPORTS 6 (2005) (GAO-05-375), available at <http://www.gao.gov/new.items/d05375.pdf>.

141. *Id.*

142. *Id.* at 7.

143. *Id.*

144. *Id.* at 11-12.

145. *Id.* at 22-24. Factors such as the distance between the detection equipment and the container or other cargo being screened, difficulties of devices in detecting highly enriched uranium which emits only gamma radiation which can be shielded using substances such as lead, consistency in the settings used on the detection devices, and maintenance of the detection equipment once control is handed over to the foreign country and port officials may hinder detection of smuggled materials..

ing evaluations of the initiative's progress, DOE is working with CBP. This interagency cooperation represents a necessary understanding of the need to obtain participation of foreign governments, companies, and ports in every applicable layer of container security defense. For that reason, these agencies may negotiate together for joint participation in the Megaports Initiative and CSI, given the complimentary nature of these programs—identifying high risk containers and providing necessary detection equipment for use in examining them.¹⁴⁶

DOE expects to have twenty (20) ports involved in the Megaports Initiative by 2010.¹⁴⁷ The additional resources made available for all aspects of port security in the SAFE Port Act may aid in meeting this goal.

F. *Secure Freight Initiative (SFI)*

Announced by the Departments of Homeland Security and Energy on December 7, 2006, the Secure Freight Initiative (SFI) was mandated by the SAFE Port Act and focuses on improving the ability to scan shipping containers overseas - before they depart for U.S. ports - for nuclear and radiological material.¹⁴⁸ The first phase of this initiative includes the deployment by the United States of scanning tools to detect these materials. This initial phase, which remains underway, focuses on six foreign ports: Port Qasim in Pakistan, Puerto Cortes in Honduras, Southampton in the United Kingdom, Port Salalah in Oman, Port of Singapore, and the Gamman Terminal at Port Busan in Korea.¹⁴⁹ As of April 2007, the initiative was active in Port Qasim and

146. See, e.g., Press Release, Bureau of Customs and Border Patrol, U.S., Colombia Agree to Combat Nuclear Smuggling (Dec. 7, <http://www.andyoppenheimer.com/articles/2006>), available at http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2006_news_releases/122006/12072006.xml (describing the joint negotiation and agreement entered into by both DOE and CBP with the government of Colombia for participation in both CSI and the Megaports Initiative); Press Release, Bureau of Customs and Border Patrol, Port of Cortes, Honduras Becomes 44th Container Security Initiative Port, First Central American Nation to Target and Pre-Screen Cargo to U.S. (Mar. 25, 2006), available at http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2006_news_releases/032006/03252006.xml (announcing similar joint agreement bringing the Port of Cortes into both the Megaports Initiative and CSI).

147. See News, *US Megaports Initiative to Prevent Nuclear Smuggling*, JANE'S CHEM-BIO WEB, June 8, 2005, [Jane's%20CB%20Web%20Megaports.htm](http://www.janes.com/news/2005/06/08/US_Megaports_Initiative_to_Prevent_Nuclear_Smuggling.htm).

148. Press Release, U.S. Dep't Homeland Security, DHS and DOE Launch Secure Freight Initiative, (Dec. 7, 2006), available at http://www.dhs.gov/xnews/releases/pr_1165520867989.shtm.

149. See *id.*

Puerto Cortes.¹⁵⁰ And, data retrieved from a radiation scanning system began being transmitted to CBP from Port Qasim on April 30, 2007.¹⁵¹

Though still in its infancy, SFI is a welcome addition to existing efforts to secure shipping containers. The benefit of SFI is an integral part of the layered security scheme undertaken in connection with container shipments and other issues of port security. By providing better screening technologies to ports from which shipments to the United States depart, initiatives such as CSI also become more effective.¹⁵²

V. National Strategies

Each of the programs discussed above is crucial to the security of container shipments and the global supply chain in which such shipments flow. The best security, however, relies on an overall strategy. That strategy includes assignment of the roles and responsibilities of the necessary players to implement these and other programs. In addition, continued assessment of security costs and benefits, security weaknesses, and technological advancements is crucial. The SAFE Port Act seeks to provide for such a comprehensive plan by requiring the Department of Homeland Security, in coordination with others, to “develop, implement, and update, as appropriate, a strategic plan to enhance the security of the international supply chain.”¹⁵³

This strategic plan must, at a minimum, consist of the following analysis and information:

- (1) describe the roles, responsibilities, and authorities of Federal, State, local, and tribal government agencies and private-sector stakeholders that relate to the security of the movement of containers through the international supply chain;
- (2) identify and address gaps and unnecessary overlaps in the roles, responsibilities, or authorities described in paragraph (1);

150. See Dannielle Blumenthal, *CBP Kicks Off Secure Freight Initiative*, U.S. CUSTOMS AND BORDER PROTECTION TODAY, Apr./May 2007, http://www.cbp.gov/xp/CustomsToday/2007/apr_may/secure.xml.

151. See Press Release, U.S. Customs and Border Protection, *Secure Freight Initiative Begins Data Transmission for Radiation Scanning in Pakistan (May 2, 2007)*, available at http://www.cbp.gov/xp/cgov/newsroom/news_release/052007/05022007.xml.

152. Provision of such technologies to foreign ports also helps counter claims that many container security initiatives harm poorer countries less able to put required security measures, including screening devices, in place. See generally Marjorie Florestal, *Terror on the High Seas: The Trade and Development Implications of U.S. National Security Measures*, 72 BROOK. L. REV. 385 (2007).

153. SAFE Port Act of 2006 § 201(a), 6 U.S.C. 941(a) (2007).

- (3) identify and make recommendations regarding legislative, regulatory, and organizational changes necessary to improve coordination among the entities or to enhance the security of the international supply chain;
- (4) provide measurable goals, including objectives, mechanisms, and a schedule, for furthering the security of commercial operations from point of origin to point of destination;
- (5) build on available resources and consider costs and benefits;
- (6) provide incentives for additional voluntary measures to enhance cargo security, as recommended by the Commissioner;
- (7) consider the impact of supply chain security requirements on small- and medium- sized companies;
- (8) include a process for sharing intelligence and information with private-sector stakeholders to assist in their security efforts;
- (9) identify a framework for prudent and measured response in the event of a transportation security incident involving the international supply chain;
- (10) provide protocols for the expeditious resumption of the flow of trade in accordance with section 202;
- (11) consider the linkages between supply chain security and security programs within other systems of movement, including travel security and terrorism finance programs; and
- (12) expand upon and relate to existing strategies and plans, including the National Response Plan, the National Maritime Transportation Security Plan, the National Strategy for Maritime Security, and the 8 supporting plans of the Strategy, as required by Homeland Security Presidential Directive 13.¹⁵⁴

The details of the extensive national plans addressing maritime security are beyond the scope of this article. Instructive to the discussion, however, is the initial report pursuant to the above-quoted statutory requirement, which report and strategy was issued by the Department of Homeland Security in July 2007.¹⁵⁵

Though the mere development of a “strategy” or “plan” does not appear any more than a bureaucratic exercise, it certainly forces the agencies involved to consider their current activities. The real question is whether any of these national strategies translate into successful implementation of beneficial security efforts. To the extent programs such as CSI, C-TPAT, ATS, the 24-Hour Rule, the Megaports Initiative and SFI are improved, the mere direction of constant review and analysis likely does no harm.

154. SAFE Port Act of 2006 § 201(b), 6 U.S.C. 941(b).

155. U.S. DEPT. OF HOMELAND SEC., STRATEGY TO ENHANCE INTERNATIONAL SUPPLY CHAIN SECURITY (July 2007), <http://www.dhs.gov/xlibrary/assets/plcy-internationalsupplychainsecuritystrategy.pdf>.

VI. A SECURE GLOBAL SUPPLY CHAIN FOR CONTAINER SHIPMENTS?

The various initiatives that the government is currently undertaking are an encouraging step toward securing shipping containers. By taking a layered approach - which permits greater flexibility - these initiatives appropriately emphasize the need for both security and efficiency. As participation grows in the programs discussed above, so too will security of shipping containers. And, as the agencies tasked with implementing these initiatives become more experienced in this new world of customs and industry cooperation, further improvements are inevitable.

No doubt there will be missteps along the way. The layered security approach, however, refuses to put all security hopes in one government program or focus. Instead, failures along the way are likely to be less cataclysmic.

Regardless of the good faith governmental efforts to secure shipping containers and the global supply chain, terrorist threats will remain. Consider the following scenario:

A container of athletic foot wear for a name brand company is loaded at a manufacturing plant in Surabaya, Indonesia. The container doors are shut and a mechanical seal is put into the door pad-eyes. These designer sneakers are destined for retail stores in malls across America. The container and seal numbers are recorded at the factory. A local truck driver, sympathetic to al Qaeda picks up the container. On the way to the port, he turns into an alleyway and backs up the truck at a nondescript warehouse where a small team of operatives pry loose one of the door hinges to open the container so that they can gain access to the shipment. Some of the sneakers are removed and in their place, the operatives load a dirty bomb wrapped in lead shielding, and they then refasten the door.

The drive takes the container now loaded with a dirty bomb to the port of Surabaya where it is loaded on a coastal feeder ship carrying about 300 containers for the voyage to Jakarta. In Jakarta, the container is transferred to an Inter-Asia ship which typically carries 1200-1500 containers to the port of Singapore or the Port of Hong Kong. In this case, the ship[sic] goes to Hong Kong where it is loaded on a super-container ship that carries 5000-8000 containers for the trans-Pacific voyage. The container is then off-loaded in Vancouver, British Columbia. Because it originates from a trusted-name brand company that has joined the Customs-Trade Partnership Against Terror, the shipment is never identified for inspection by the Container Security Initiative team of U.S. customs inspectors located in Vancouver. Consequently, the container is loaded directly from the ship to a Canadian Pacific railcar where it is shipped to a rail yard in Chicago. Because the dirty bomb is shielded in lead, the radiation portals currently deployed along the

U.S.-Canadian border do not detect it. When the container reaches a distribution center in the Chicago-area, a triggering device attached to the door sets the bomb off.¹⁵⁶

This scenario was provided during a congressional hearing prior to enactment of the SAFE Port Act. This latest legislation, to some extents, attempts to correct some of the potential security breaches highlighted by this hypothetical terrorist plot.

Just as this terrorist dirty bomb scenario highlights the different links in the global shipping supply chain subject to infiltration by terrorists, recommendations made to reduce the risk of such infiltration have guided, at least in part, many of the changes effected by the SAFE Port Act. Implementation of this legislation and recent CBP and DOE efforts seek to improve container tracking capabilities and to provide methods for more thorough container screening. These efforts continue to move container security strategy in the right direction. No doubt more work remains.

Ultimately, some of the success in this arena will depend upon advancements in technologies that can be made available at reasonable prices.

Security technology is continuously evolving, not only in terms of capability but also in terms of compatibility, standardization, and integration with information systems. It is important to note that there is no single technology solution to improving supply chain security. As technology matures, it must be evaluated and adjustments to operational plans must be made. Priority should be given to effective security solutions that complement and improve the business processes already in place, and which build a foundation for 21st century global trade. A more secure supply chain also can be a more efficient supply chain.

.....

Technology plays a particularly important role in providing for screening of cargo at the critical nodes of the supply chain through data acquisition, delivery, and analysis (e.g., the secure transmission of cargo manifests). It also provides for certainty, through scanning and imaging of cargo at those nodes where multiple cargo flows join, (e.g., at ports of departure and entry). Such information built into normal business process as a preventative measure also leverages recovery

156. Flynn Testimony 2, *supra* note 19. Though this scenario was used to highlight weaknesses in container shipment security prior to enactment of the SAFE Port Act, it cannot be expected that the legislation removed all of the opportunities for terrorist infiltration into container shipping routes. What is notable is the attention paid to some of the weaknesses exposed by this hypothetical operation in crafting container security programs.

capabilities by providing necessary information to key decision makers on the safety, security and prioritization of cargo.¹⁵⁷

Better technologies may permit more efficient cargo screening and examinations of a larger number of containers, ideally, prior to departing for and entering United States ports. Certainly, a continued focus on technology is appropriate.

CBP is currently utilizing large-scale X-ray and gamma ray machines and radiation detection devices to scan cargo. The acquisition and deployment of radiation detection equipment is coordinated closely with DHS' Domestic Nuclear Detection Office (DNDO). Presently, CBP operates over 913 radiation portal monitors (RPMs) at our Nation's ports (including 342 RPMs at seaports), utilizes over 180 large scale non-intrusive inspection devices to examine cargo, and has issued 14,150 handheld-held radiation detection devices. DNDO is currently developing next-generation technologies for CBP and other operators that will provide improved detection capabilities. These next-generation systems will be gradually introduced at our nation's ports beginning this calendar year. Also, over 600 canine detection teams capable of identifying narcotics, bulk currency, human beings, explosives, agricultural pests, and chemical weapons are deployed at our ports of entry.¹⁵⁸

Non-intrusive inspection devices are assuredly key to quick container examination. Equally important is the use of devices to detect intrusion into containers so that those containers passing inspection at the time of loading are not tampered with in route to the United States. In a perfect world such devices would detect the unauthorized intrusion anywhere on a container and not just intrusions through the container doors. "[J]ust because you have a device that secures the doors does not mean that the container is secure."¹⁵⁹

Technology alone, however, will never provide the entire security solution. Moreover, the costs of newer technologies may outweigh their benefits and may often be cost prohibitive for some participants in the global shipping market.

The lesson to be learned from recent developments in securing shipping containers is that there is no one solution - no single answer. The answers lie in what the government seems to have realized: it is a

157. U.S. DEPT. OF HOMELAND SEC., STRATEGY TO ENHANCE INTERNATIONAL SUPPLY CHAIN SECURITY 28 (2007), <http://www.dhs.gov/xlibrary/assets/plcy-international-supplychainsecuritystrategy.pdf>.

158. DHS Preliminary Report, *supra* note 115, at 76.

159. *CBP Chief Wants Total Container Security Device*, DEFENSE DAILY INT'L, Jan. 3, 2007, <http://www.securityinfowatch.com/online/The-Latest/CBP-Chief-Wants-Total-Container-Security-Device/10168SIW306>.

number of complementary approaches, used together, that provides the best method of protection. Resisting the temptation to rely on a single, all-encompassing solution is most likely to prevent unacceptable economic results, and most likely to keep our enemies guessing and prevented from undermining our security.