Chapter 5: Cargo Security

Steven W. Baker

Steven W. Baker is the principal of the Law Offices of Steven W. Baker. He has specialized in the practice of Customs and International Trade Law in the San Francisco Bay Area for over thirty-five years. He is a past Chair of the Customs Law Committee, Section of International Law, American Bar Association, and is active in many bar and trade associations, including the American Association of Exporters and Importers.

5.1 Introduction

The United States Customs Service was created by Congress in 1789. At that time, Customs' primary function was "protection of the revenue" (i.e., collection of duties). Over the next 200+ years, Congress gave Customs myriad other responsibilities, including: narcotics interdiction, export control, investigation of money laundering and intellectual property infringement; enforcement of product labeling requirements, quarantines, and restrictions; collection of taxes and fees for other agencies; administering trade restraints, including dumping, countervailing duties, and tariff rate quotas; and evaluation and quantification of trade information both for trade enforcement and the collection of import and export trade statistics for the Census Bureau. Through it all, however, Customs' primary responsibility remained revenue protection until the major restructuring of many government functions in the wake of 9/11.

In March 2003, the U.S. Customs Service was transferred from the Department of the Treasury to the new Department of Homeland Security and renamed U. S. Customs and Border Protection (CBP). In addition to its revenue protection mandate while also "securing and facilitating trade and travel" and "enforcing hundreds of U.S. regulations, including immigration and drug laws," CBP now has "a priority mission of keeping terrorists and their weapons out of the U.S." The Border Patrol, the Animal and Plant Health Inspection Service of the Department of Agriculture, and the inspection function of the Immigration and Naturalization Service were all transferred into the renamed agency, making CBP the primary border security agency of the United States.

The element of the new anti-terrorism function of CBP that most directly impacts importers into the U.S. is the emphasis on supply chain security. Prior to 9/11, cargo security primarily involved drug interdiction efforts and actions against smuggling. Numerous programs have now been and continue to be developed to implement the goal of keeping terrorists and their weapons from infiltrating the merchandise supply chain. These include partnership programs, the use of advance data acquisition and targeting tools, and physical controls.

Four major initiatives discussed in the next four sections illustrate the approaches CBP has taken to upgrading cargo security:[i]

5.2 C-TPAT

The Customs-Trade Partnership Against Terrorism (C-TPAT) was initiated by then-Customs Commissioner Robert C. Bonner even before the restructuring of the agency in 2003. A voluntary program initially open only to importers, it has been expanded to include most participants in international supply chains. Customs brokers, carriers, warehouses, ports and terminal operators, third party logistics suppliers (3PLs) and consolidators, and, with certain limitations, foreign suppliers can now all participate.

The benefits of participation depend on the "tier" compliance level of the participant. In general, import shipments of C-TPAT members are 4-6 times less likely to be examined for security or enforcement purposes, and, if selected, go to the head of the line for exam. Members are promised priority of entry following any major trade disrupting event and have access to supply chain specialists and training and workshops. There are documented "intangible" benefits of increased supply chain efficiencies following the development of a security profile and adoption of "best practices," as well as the satisfaction of joining in the fight against terrorism.

Interested participants must apply for membership, which involves providing corporate information, preparing a Security Profile for the company including security information for suppliers or other supply chain members, and agreeing to voluntarily participate. Minimum security criteria have been developed for each class of participant, and CBP recommends use of the 5 Step Risk Assessment Process to develop the necessary information.

The 5 Step Risk Assessment Process includes:

1. Mapping cargo flow and identifying business partners (directly or indirectly contracted)

2. Conducting a threat assessment focusing on: terrorism, contraband smuggling, human smuggling, organized crime, and conditions in a country/region which may foster such threats and rating threats as High, Medium, Low

3. Conducting a vulnerability assessment in accordance with C-TPAT Minimum Security Criteria and rating vulnerability – High, Medium, Low

4. Preparing an Action Plan

5. Documenting how risk assessments are conducted

Once an application is accepted, each participant must be validated through an on-site visit from CBP supply chain specialists, and, where appropriate, a visit to one or more foreign suppliers to verify the data submitted. Annual updates to the Security Profile must be filed, and re-validations, including additional foreign vendor visits, may be scheduled.

The U.S. C-TPAT program became the model for the Authorized Economic Operator (AEO) concept included in the World Customs Organization's *Framework of Standards to Secure and Facilitate Global*

Trade. The U.S. has entered into or is in negotiation for mutual recognition agreements with Canada's Partners in Protection (PIP) and similar AEO programs in the EU, New Zealand, Japan, Korea, Jordan, and Singapore. Companies that are accepted as validated members of the programs in the mutual recognition agreement (MRA) countries will receive the benefits of C-TPAT membership in the U.S., and C-TPAT members will be afforded AEO or equivalent status in the MRA countries without having to reapply under each county's requirements.

Although a voluntary program with (as of this writing) only slightly more than 10,000 members, about 40% of which are importers (compared to more than 400,000 importers of merchandise into the U.S. in an average year), C-TPAT covers over 50% (by value) of all imported goods, due to the participation of a high percentage of the largest importers. Many of these importers require their supply chain participants, such as carriers, warehouses, and brokers, to be C-TPAT members as well, thereby reducing the burden of updating Security Profile information and ensuring participation at a higher tier level.

5.3 CSI

The Container Security Initiative (CSI) is the second major cargo security initiative from CBP. This program involves cooperation between CBP and foreign governments, "moving the borders outward" to conduct cargo screening in the ports of lading before shipments ever leave for the U.S. Although CSI covers only maritime containerized cargo, more than 90% of all manufactured goods worldwide move in containers, with 40% of those traveling by sea. Currently the program pre-screens over 80% of all containerized maritime cargos shipped to the U.S.

CSI has placed U.S. CBP officers in 58 ports located in more than 30 countries. Working with the host governments, these officers identify high risk containers through targeted screening procedures based on advance cargo data, and pre-screen the containers prior to shipment. The screening process involves the use of high tech tools, including X-ray and gamma-ray scanners and radiation detectors, with physical inspection of cargos where circumstances warrant.

The CSI screening process has been supported by the EU, the WCO, and the G8 countries for use at ports throughout the world.

5.4 Mandatory Advanced Electronic Cargo Information

The Trade Act of 2002 established requirements for carriers to supply cargo manifest information in advance of the entry of goods into the U.S. CBP began implementation with maritime cargo, often called the "24 Hour Rule" after the time period required for filing container cargo manifest data prior to the loading of the container on the vessel in the foreign port. Break-bulk cargo is subject to reporting 24 hours prior to *arrival* in the U.S.

The program has now been expanded to cover all types of carriers, including air, rail, and truck carriers, with the amount of prior reporting time dependent on the nature and the type of carrier, the length of the trip, and in some cases whether the carriers (and sometimes the shippers) are participants in related cargo security programs. The information received is used in part for CSI targeting purposes and in part to identify shipments which CBP believes warrant further scrutiny after arrival in the U.S.

Implementation of these requirements has necessitated greater, and much earlier in the supply chain, cooperation between the shipper and/or importer and the carrier or carriers involved. Cargo that has not been included on an Advanced Manifest may be refused permission to load, and problems in matching the Bills of Lading for notified merchandise with the Vessel Manifest can create serious issues. Despite high levels of concern as the various requirements for different modes of transportation went into effect, the glitches were worked out, and cargo continued to move under the new systems.

5.5 Importer Security Filing (ISF)

Advance data reporting requirements have been extended to importers as well as carriers through the Importer Security Filing (ISF), originally identified as “10+2” based on the number of required data elements. All importers must file electronic information prior to importation, except for certain bulk cargo shipments. The data must be supplied on varying time schedules similar to the Advanced Cargo Information rules. The requirement is so far limited to maritime cargo.

The ISF must include identifying information regarding the manufacturer/shipper, the importer, the consignee, and the cargo, including such details as HTSUS number, the country of origin, and the name and location of the container stuffing agent. The “+2” refers to the two data elements that must be supplied by the carrier -- the vessel stow plan and container status message.

Importers are required to file surety bonds (like those used to secure duties and fees) covering the filing, with the possibility of incurring liquidated damages for late or missing filings. Containers for which ISFs have not been filed may be denied lading on a vessel or refused entry into the U.S. on arrival.

The data gathered is transmitted to the National Targeting Center and used to identify cargo shipments that warrant special or further examination or handling by CBP. The program extends the distance from arrival in the U.S. that supply chain information must be gathered and processed for submission to CBP, and requires importers in many cases to become involved in areas (such as container stuffing) that have not previously been closely reviewed. This program was also thought likely to involve great difficulties for importers in the securing of information and in creating the risk of substantial disruption of cargo shipments, but has been implemented without major difficulties.

5.6 Risk Management

A common component of all of these programs is the use of risk management principles. Risk management is defined as "a proactive management technique that identifies processes for controlling risk in trade compliance." CBP embraced risk management in the 1990’s in connection with enforcement of commercial requirements (proper classification valuation, marking, etc.). The principles were quickly adopted for cargo security activities after 9/11.

CBP lists the four components of risk management as: collecting data and information, analyzing and assessing the risk, prescribing action and dedicating the necessary resources, and then tracking and reporting the results of that action. These principles are incorporated in each of the programs discussed above, as well as many others, and are used to identify areas of concern and allocate resources so as to maximize their effect. In conducting this process, Customs defines risk as "the degree of exposure to the chance of noncompliance which would result in loss or injury to trade, to industry, or the public."

CBP no longer has the resources to physically examine at least a portion of every shipment entered into the U.S., as it was mandated to do just fifty years ago before the explosion of trading volumes. It does, however, secure information about, analyze, and employ risk management procedures with regard to every shipment. Multiple programs, both voluntary and mandatory, involving "trusted partners," sophisticated data mining, and technology-based force multipliers allow CBP to determine levels of risk and apply its resources to manage and reduce those risks. Physical controls including the use of radiation portals and handheld radiation monitors, upgraded standards for container security seals, and the deployment of non-intrusive scanning equipment are in place; and discussion of such possible additional programs as container intrusion detection equipment and RFID tracking systems is in progress. Leveraging the efforts of trade partners, such as C-TPAT members and the equivalents in mutual recognition countries, allows CBP to extend its reach along the supply chain. Ever-expanding targeting abilities based on increasing data input permits focusing resources on clearly identified areas of concern.

5:7 Conclusion

CBP is adding and expanding programs to address security concerns, such as the Beyond the Border Action Plan with Canada and the Air Cargo Advance Screening Initiative. The agency's emphasis on supply chain security as a methodology for protecting the U.S. against the infiltration of terrorists and their weapons into the US continues to place additional burdens and responsibilities on all parts of that supply chain. Importers who fail to take sufficient steps to understand, monitor, and control their entire logistics chain will likely face increased Customs cargo exams, reviews, audits, and delays in clearance of their shipments.

[i] Each of these programs is discussed in more detail under the Cargo Security section of the Trade tab on CBP's website, www.cbp.gov.