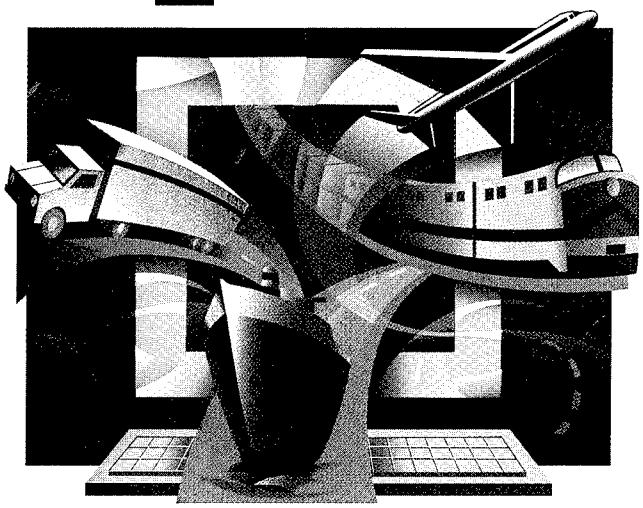
# INTERMODAL CARGO TRANSPORTATION



PB99-152761

## INDUSTRY BEST SECURITY PRACTICES

REPRODUCED BY
U.S. DEPARTMENT OF COMMERCE
NATIONAL TECHNICAL
INFORMATION SERVICE
SPRINGFIELD, VA 22161

MAY 1999

## About the National Science and Technology Council

President Clinton established the National Science and Technology Council (NSTC) by Executive Order on November 23, 1993. This cabinet-level council is the principal means for the President to coordinate science, space, and technology policies across the Federal Government. NSTC acts as a "virtual" agency for science and technology (S&T). The President chairs the NSTC. Membership consists of the Vice President, Assistant to the President for Science and Technology, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

Through the NSTC, Federal departments and agencies work cooperatively to ensure that Federal science and technology investments support national goals. NSTC Committees prepare R&D strategies that are coordinated across the Federal Government to form a comprehensive investment package.

Call 202-456-6102 to obtain additional information regarding the NSTC.

## About the National Science and Technology Council

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization and Priorities Act of 1976. OSTP's responsibilities include advising the President in policy formulation and budget development on all questions in which science and technology are important elements; articulating the President's S&T policies and programs; and fostering strong partnerships among Federal, State, and local governments, and the scientific communities in industry and academe. The Director of OSTP also serves as Assistant to the President for Science and Technology, and manages the NSTC for the President.

Call 202-395-7347 to obtain additional information regarding the OSTP or see our web site at:

http://www.whitehouse.gov/WH/EOP/OSTP/html/OSTP_Home.html

Prepared by:
United States Department of Transportation
Research and Special Programs Administration
John A. Volpe National Transportation Systems Center
55 Broadway
Cambridge, Massachusetts 02142

For specifics about this study contact Principal Investigator:
John J. Publicover Jr. at 617-494-3301

**Technical Report Documentation Page**

| 1. Report No. | 2. Government Accession No. | 3. Rec |
|---|---|---|
| DOT-T-99-19 | | PB99-152761 |

| 4. Title and Subtitle | 5. Report Date |
|---|---|
| INTERMODAL CARGO TRANSPORTATION: INDUSTRY BEST SECURITY PRACTICES | May 1999 |
| | 6. Performing Organizational Code |
| 7. Author(s) | 8. Performing Organization Report No. |
| 9. Performing Organization Name and Address<br>U.S. Department of Transportation<br>Research and Special Programs Administration<br>John A. Volpe National Transportaton Systems Center<br>55 Broadway<br>Cambridge, MA 02142 | 10. Work Unit No. (TRAIS) |
| | 11. Contract or Grant No. |
| 12. Sponsoring Agency Name and Address<br>U.S. Department of Transportation's Technology Sharing Program<br>400 Seventh Street, S.W., Room 8417<br>Washington, DC 20590 | 13. Type of Report and Period Covered<br>May 1999 |
| | 14. Sponsoring Agency Code<br>**DOT/RSPA** |

15. Supplementary Notes

**Released in cooperation with the U.S. Department of Transportation's Technology Sharing Program**

16. Abstract

This report provides the results of research, interviews and on-site evaluations conducted to identify issues related to security of cargo terminals to theft, smuggling, and other illegal activity. This report also provides industry best security practices for eliminating, mitigating, and controlling identified concerns within the security framework of cargo transportation. In keeping with the transportation infrastructure assurance philosophy, this report is not organized by mode (truck, rail, maritime, and pipeline), but rather provides and integrated discussion of all modes using cargo terminals with a special focus on intermodalism.

| 17. Key Words | 18. Distribution Statement |
|---|---|
| Transportation; Cargo; Security; Intermodal; Theft; Smuggling | **Availability is unlimited. Document is being released for sale to the U.S. public through the National Technical Information Service, Springfield, Virginia 22161** |

| 19. Security Classif. (of this report) | 20. Security Classif. (of this page) | 21. No. of Pages | 22. Price |
|---|---|---|---|
| **Unclassified** | **Unclassified** | 104 | |

# Intermodal Cargo Transportation:

# Industry Best Security Practices

## May 1999

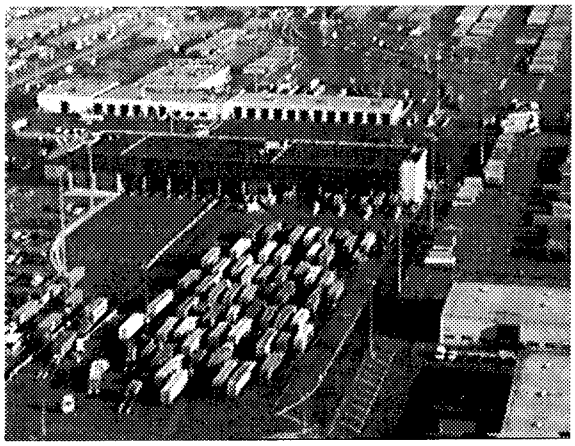
# Table of Contents

# List of Figures



# List of Tables

# Intermodal Cargo Transportation: Industry Best Security Practices



## 1. Introduction

Cargo-related crimes, including cargo theft, insurance fraud, drug trafficking, and the transportation of illegal immigrants into the United States, have all become dominant criminal issues on the national agenda. Concentrated government efforts attempt to combat cargo-related crimes; however, organized criminal activity continues to grow in both frequency and consequence. Increasing violence and criminal penetration of transportation operations and technologies significantly compromise the U.S. transportation infrastructure.

In recognition of the importance of addressing this problem, a ***Transportation Infrastructure Assurance Initiative*** was included among the thirteen specific Partnership Initiatives delineated in the National Science and Technology Council (NSTC) *Transportation Science and Technology Strategy*, prepared by the Transportation R&D Subcommittee of the NSTC Technology Committee. The Department of Transportation's Research and Special Programs Administration, working through its Volpe National Transportation Systems Center (Volpe Center), has served as the executive agent for the initiative. This report is the first product of the initiative, which is aimed at improving industry capabilities to detect and control criminal activity at cargo terminals. More broadly, the focus is on developing and implementing means of improving the overall security of passenger and freight terminals, as well as of the people and cargo transiting these locations.

This report represents the results of research, interviews and on-site evaluations conducted to identify the issues related to security of *cargo terminals* to theft, smuggling, and other illegal activity. This report also provides industry best security practices for eliminating, mitigating, and controlling identified concerns within the security framework of cargo transportation. In keeping with the *transportation infrastructure assurance* philosophy, this report is not organized by mode (truck, rail, maritime, and pipeline), but rather provides an integrated discussion of all modes using cargo terminals with a special focus on intermodalism.

## Transportation Infrastructure Assurance

Cargo transportation, with the inherent dynamics of an intermodal environment, faces increased and complicated opportunities for theft, pilferage, and smuggling. Discussion of these opportunities within the transportation industry historically has been splintered by modal differences that often dictate competing priorities and specialized views. In contrast, transportation infrastructure assurance requires the application of a *systems approach* to the identification and resolution of cargo terminal security. This approach is defined as:

> "The application of operating, technical, and management techniques and principles to the security of a facility throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources."

Transportation infrastructure assurance advocates a form of risk management that eliminates or controls threats and vulnerabilities through an ongoing resolution process. This approach identifies, evaluates, and controls security threats and issues specific to security through all system life cycle phases, including terminal design, construction, operation, replacement, and disposal. This proactive approach encourages both the design and installation of features which "harden" terminal elements against criminal activity, and the implementation of security information monitoring systems, which identify and control new threats and security concerns. During all life-cycle phases, the terminal is assessed as an integrated system, rather than a collection of modal transfer and storage hubs.

A security program utilizing this approach offers the functional and integrated capability of protecting users and operators, as well as the resources of the terminal. The basic elements of protection involve prevention or deterrence of acts or conditions threatening the safety or welfare of those persons or resources, and corrective or remedial action to limit the effects of such acts or conditions when they do occur.

Efforts to gather data and information included (Appendix A):

- Distribution of a series of questions to major ports, and shippers.
- Correspondence with trade associations soliciting their input.
- Correspondence with and solicitation of input from Federal Government agencies with primary law enforcement and border integrity responsibilities.
- Correspondence and interaction with underwriters and industry groups.
- Cooperation with the National Cargo Security Council, the American Trucking Association, American Society for Industrial Security, and the Technology Asset Protection Association.
- On-site inspection, interview, and analysis.
- Literary and Internet searches.

This report applies systems analysis to identify issues related to security of interfaces between surface and marine modes, and does not focus on air terminals or its cargo. Aviation cargo security is being addressed separately as part of Vice President's Commission on Aviation Safety and Security (see http://www.aviationcommission.dot.gov/index.html).

Additionally, this report identifies issues related to criminal activity, and recommends coordinated and integrated countermeasures to be supported by the Federal Government and implemented by industry.

## Organization of Report

This report is organized into four areas. The first describes introductory information and definitions. The second discusses results of research conducted to assess the extent of criminal activity in the transportation industry, and more specifically, at cargo terminals. The third area presents the results of on-site evaluations and interviews conducted to identify specific issues related to security at cargo terminals around the country. Finally, the report provides industry best practices and recommendations to reduce the vulnerability of cargo terminals to criminal activity. Included as well are conclusions and recommendations for further analysis.

# 2. Research Findings: Cargo Crime and Cargo Terminal Concerns

The effective operation of the U.S. economy and the protection of the Nation depend on efficient movement of people, goods, information, and financial resources. This movement is assured by the U.S. transportation infrastructure, an interdependent and interconnected system of highways, railways, waterways, pipelines, and airports. Cargo terminals provide the "heart" of this transportation network, facilitating the organized and efficient transfer of cargo between or among modes, and preparing it for delivery to final destinations.

This section presents research findings concerning the two most significant threats to the operation of cargo terminals: cargo theft and fraud and drug trafficking.

## Cargo Theft

Cargo theft from terminals interrupts the smooth functioning of the U.S. distribution system, and first received considerable research attention in the late 1970s and the early 1980s. Prompted by changing patterns in theft, government and private industry analysts attempted to quantify the extent of cargo theft throughout the Nation.

In March 1980, on the eve of major transportation deregulation legislation, the General Accounting Office (GAO) released a study identifying the extent of cargo crime in the United States and evaluating the performance of the USDOT Office of Transportation Security (OTS) in quantifying and addressing this crime. Subsequent motor carrier, rail, and international shipping deregulation rendered reporting changes that severely limited OTS's ability to collect data on the extent of crimes committed against transportation carriers. As a result of these changes, the GAO study remains one of the most comprehensive evaluations of cargo crime to date.

This study found that cargo theft in the transportation network "disrupts the reliable and efficient flow of goods from shippers to receivers. It is also expensive; theft-related losses, which include the direct cost of the stolen cargo, higher insurance premiums, and additional administrative expenses, reduce transportation industry profits and increase prices for consumers."[1]

Based on reports from the Interstate Commerce Commission (ICC), the Civil Aeronautics Board (CAB), the Federal Maritime Commission (FMC), and Quarterly Freight Loss and Damage submissions by major regulated motor carriers and railroads, OTS estimated that 1977 losses experienced as a result of cargo theft amounted to approximately $1 billion.[2] (When adjusted for inflation, the GAO figure equals approximately $1.8 billion in 1997 dollars.) According to OTS data, direct costs by mode were estimated as follows:

---

[1] Report by the Comptroller General of the United States, General Accounting Office, "Promotion of Cargo Security Receives Limited Support," Washington, D.C., 1980, p. 1.
[2] GAO, p.11.

- Motor Carriers: $870 million
- Maritime: $80 million
- Rail: $41 million
- Air: $7 million
- Other: $2 million (See Figure 5)[3]

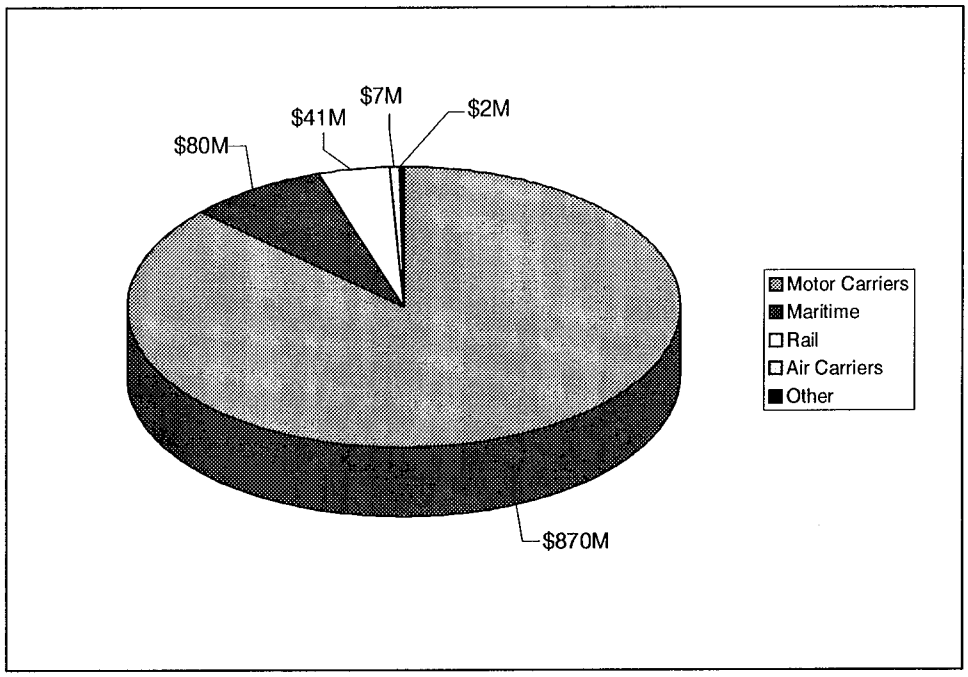



**Figure 1: 1977 OTS Cargo Theft Estimates by Mode**

Indirect costs, such as filing, investigating, and paying claims, were believed to be two to five times the amount of losses, bringing the total cost estimated by OTS to between $2 and $5 billion.[4] The majority of this theft occurred at cargo terminals and terminal transfer facilities.

Based on an independent review of the 1977 data, the GAO determined that OTS analysis "understated the amount of theft-related losses."[5] GAO found that the OTS data relied exclusively on submissions from large carriers (in some cases, medium and small carriers were not even aware of OTS cargo theft data collection activities), and because of limited reporting requirements, did not appropriately integrate cargo theft data from the insurance industry.

Further, according to the GAO, OTS analysis did not address the issue of unreported or under-reported losses. According to the GAO, shippers and insurance companies were reticent about reporting losses that could result in publicity and inhibit customer confidence. As a result, the transportation industry often viewed it as less costly to absorb smaller claims and have insurance cover larger claims. Additional rationales for under-reporting identified by the GAO include:

- Carriers frequently feared that shippers might shift business to another carrier due to security concerns.

- Carriers wanted to limit the ability of competitors to disclose their security record as part of efforts to gain market share.

[3] GAO, p.11.
[4] GAO, p.11.
[5] GAO, p.11.

- Carriers feared that insurance companies would use theft statistics to justify increased premiums for coverage.

- Carriers were unable to determine the actual point of loss during a long or complex trip.[6]

## Cargo Theft Today

The Federal Bureau of Investigation (FBI) conservatively estimates that cargo theft-related incidents account for $3.5 billion in merchandise losses in the United States annually. This estimate is based primarily on data obtained from local law enforcement agencies with significant cargo theft-related losses. However, the rule of thumb used by law enforcement in estimating property theft is that only 40 percent of businesses or individuals actually report the theft. Based on this percentage the FBI estimate equates to $8.75 billion for 1997. The FBI readily acknowledges that this estimate may not reflect the losses of smaller transportation facilities and cargo stolen in regions not affiliated with the FBI's cargo criminal apprehension programs or task forces.[7]

The National Cargo Security Council (NCSC), a coalition of public and private transportation organizations, estimates that cargo theft accounts for more than $10 billion in merchandise losses each year. This estimate is based on confidential data provided to the NCSC by transportation freight carriers and insurance groups, and may be more inclusive than the FBI assessment. Figure 2 presents the twenty-year trend for direct losses from cargo theft.

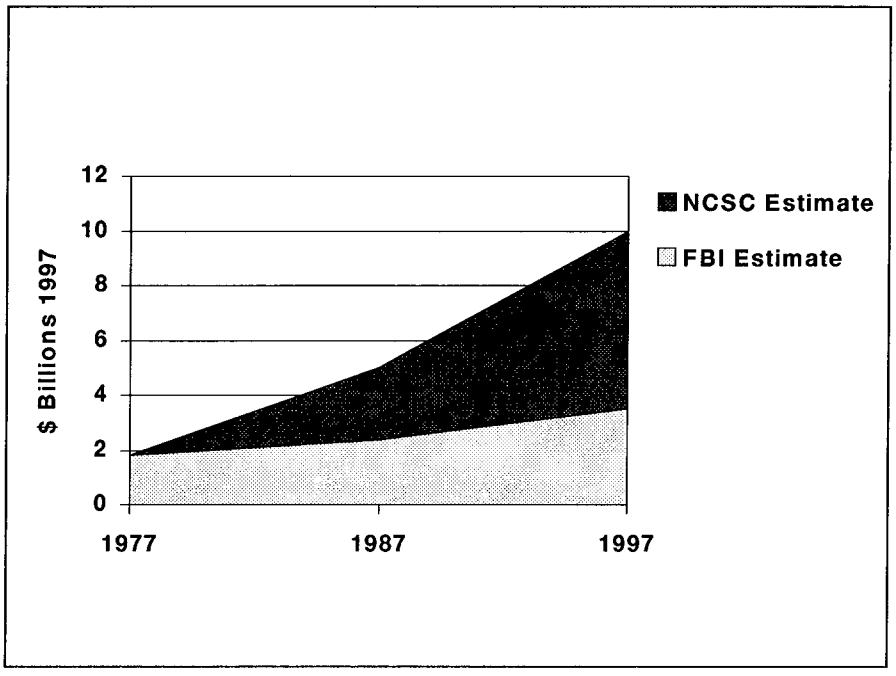



**Figure 2: FBI and NCSC Cargo Theft Estimates (Twenty-Year Trend)**

[6] GAO, p.12.
[7] American Trucking Association and Federal Bureau of Investigation interviews.

The NCSC estimate is a composite number and is not broken down by annual losses for mode of freight transportation. Many analysts believe that motor carriers experience the majority of loss due to cargo theft (approximately 85 percent of all reported thefts), followed by maritime, rail, and air.[8] This is not surprising since, in terms of value, nearly three-quarters of all cargo is transported by truck, followed by postal, parcel, and courier service, rail, and water. *While cargo loss can be attributed to individual modes, both the FBI and NCSC estimates indicate that the majority of cargo theft actually occurs in cargo terminals, transfer facilities, and cargo consolidation areas.*

The costs of stolen merchandise are not the only losses associated with cargo theft. When applying the conservative multiplier identified in the GAO study to determine indirect costs of cargo theft, total costs are estimated at between $20 billion and $60 billion per year. This figure includes the cost of filing, investigating, and paying claims, but does not include all law enforcement and security technology expenses.

## Containerized Cargo Crime

The "container revolution," which has increased transportation efficiency and spawned the rapidly growing intermodal freight transportation industry, may have inadvertently encouraged increased organized criminal presence in freight transportation.

Traditionally (before the 1960s), high-value cargo was moved using break-bulk packaging and shipping techniques. During the "break-bulk" era, high-value cargo was packaged in cases or pallets for shipment and loaded and unloaded on a piece-by-piece or pallet-by-pallet basis. Easy access encouraged the theft of electronics, appliances, clothes, engine parts, liquor, cosmetics, and cigarettes from terminals (including warehouses, docks, and transfer points) and during loading, unloading, and shipment.

During the 1950s, high levels of pilferage from break-bulk shipments, combined with promises of increased efficiency, encouraged the U.S. military to experiment with containers. First used by military traffic commands, containers were extended to commercial use in the mid-1960s. Container use has continued to grow steadily in the United States and is projected to grow at 6 percent annually. Presently, 80 percent of U.S. overseas cargo trade is containerized. Over 60 percent of the world's deep-sea general cargo is transported in containers. Worldwide, more than 400 ports have the capability to handle containers.

Containers have become the primary means for shipping cargo between economically strong and stable countries. Along these trade routes, containerization of cargo approaches 100 percent. Containerized shipping is crucial in routes across the North Atlantic, and between the United States and Japan and neighboring countries. The technology and capital investments required to load, ship, store, and unload containers, however, limit their use on routes involving Less-Developed Countries (LDCs). In these markets, cargo is usually shipped according to the non-containerized classifications of bulk, break-bulk, and neo-bulk.

---

[8] Barry M. Tarnef quoted in "Security of U.S. Ports Challenged by Thieves, Smugglers, and Terrorists" by Carlos J. Salzano in *Traffic World*, September 25,1989.

Terminals to handle transported containers require more land for storage and transfer than do break-bulk or bulk terminals. Containers have received wide acceptance in the transportation industry, however, because of their numerous benefits in operating efficiency, including:

- Goods can be handled in less time, utilizing fewer personnel.
- Goods are better unitized and protected during shipment.
- More goods can be shipped in a "unified" package that does not need to be transloaded at ports or terminals, but can be shipped directly to the destination.
- Record keeping is simplified.

When first introduced, containers successfully reduced pilferage. Estimates indicated that during the early years of the container revolution, theft of containerized cargo dropped to less than one-tenth of 1 percent of all cargo shipped in containers.[9] Unfortunately, "after an initial honeymoon period, during which criminals adjusted to the new container system, other patterns of theft developed."[10]

Organized crime recognized the potential for big business. Containers, stacked in terminals, could be stolen as a whole, opened and made subject to pilferage, or serve as a conduit for drug smuggling. "Much larger 'packages' containing higher value cargoes could now be spirited away with comparative ease and the spoils made it worth using more elaborate methods of deception and daring. Whereas, previously ten televisions might go missing because that was all thieves could carry or secrete, now two hundred could be stolen at a go in a container." [11] For example, computer laptops, cellular telephones, perfume, and wearing apparel are among the top items stolen and could be worth from hundreds of thousands of dollars to millions of dollars per container load. A pallet of these devices can command upwards of $250,000. Sixty-four pallets can be loaded into a single 40-foot container, with a net value of $16 million.[12]

Based on new patterns of cargo theft, the U.S. Coast Guard, the NCSC, and American Trucking Association (ATA) estimate that the value of single cargo thefts is on the rise, averaging approximately $500,000 in 1996. This estimate represents a five-fold increase from 1970.[13]

## Methods of Cargo Theft

Containerized cargo theft is carried out primarily as an organized criminal conspiracy. Substantial evidence supports the hypothesis that most theft of containerized cargo is systematic in method.[14] Often, criminals act with apparent information about cargo manifests, suggesting that collusion is occurring with transportation employees. Cargo terminals are particularly

---

[9] Gerhardt Muller, Intermodal Freight Transportation, 3rd Edition, Lansdowne, Virginia: Eno Transportation Foundation, Inc., 1995, p.164.
[10] Barry Tarnef, as quoted in "Security at U.S. Ports Challenged by Thieves, Smugglers, and Terrorists."
[11] Roy Campbell, "Study in Crime," Cargo Systems, May 1991.
[12] MaryLu Korkuch, "High Tech Cargo Theft: A Presentation to the U.S. Capital," April 9, 1996.
[13] American Trucking Association interviews.
[14] Morelli, Thomas D., A Data Base of Containerized Maritime Cargo Theft Incidents: A Strategic Tool for Reducing Vulnerability, U.S. Department of Transportation, Washington, DC.

vulnerable to employee penetration at intermodal transfer points, warehouses, rail yards, and docks. In its *Ports of the World: A Guide to Cargo Loss Control*, the CIGNA Corporation reports that the majority of cargo loss claims "involve cargo taken from transportation facilities by personnel authorized to be there and on vehicles controlled or similarly authorized by management."

This immense network of importers, wholesalers, freight brokers, truckers, and dock workers create problems for law enforcement and transportation operations in pinpointing instances of bribery, extortion, or "purchased" information. Estimates indicate that "well over 80 percent of all theft and pilferage of transportation cargoes is accomplished by, or with the collusion of, persons whose employment entitles them access to the cargo that is stolen."[15]

Criminals use a variety of methods to steal cargo, including:

- Opening containers stacked at terminal yards or transfer facilities, removing goods, and transporting them from ports or intermodal facilities by personal automobile or delivery trucks.

- Falsely claiming that a truck was hijacked leaving a port or warehouse, when the driver is actually complicit in the crime, and receiving a cut of the profits.

- Dismantling containers, removing key merchandise, re-sealing containers and continuing shipment

- Relying on an organized network for spotting, stealing, and fencing merchandise.

- Driving off in a loaded tractor trailer via fraudulent paperwork

- Speeding through fences and security checkpoints.

- Stealing loaded trucks off the street or from storage yards.

Once stolen from a terminal, the cargo merchandise is quickly repackaged in a nearby warehouse or facility for transportation to an out-of-state fencing location or out of the country. These goods may re-enter the United States and be sold at a discount, providing an effective way to legitimize illegal profits (referred to as transshipment). The FBI estimates that most stolen cargo remains in the possession of those who stole it for less than twenty-four hours.

Organized criminal groups are becoming transnational, facilitating theft of containerized cargo in one country and trafficking of stolen goods in another. Transnational criminal operations use the entire international shipping cycle, in particular, the maritime and trucking transportation shipping system and the freight-forwarding sector, to support stolen merchandise trafficking.

[15] United Stated Department of Transportation, "A Report to the President on the National Cargo Security Program, "Washington, DC, March 1980.

Organized criminals enjoy the same efficiencies and economies of scale as legitimate transnational businesses, but can elude national efforts to restrict their activities.[16]

## Regional Patterns in Cargo Theft

The FBI estimates that $1 to $2 million worth of cargo theft occurs daily in three regions of the country, accounting for approximately three-quarters of the FBI's estimate for the Nation's total cargo theft. Since 1994, specialized cargo units in these three regions, comprised of local law enforcement and the FBI, have made thousands of arrests and recovered hundreds of millions of dollars in stolen property.[17]

The FBI estimates that more than $1 billion worth of cargo is stolen annually in the New York/New Jersey area alone, which has the Nation's most active trucking, rail, and continual freight handling system. [18] Local law enforcement agencies in Southern California estimate that approximately $500 million worth of cargo is stolen annually in their region.[19] Federal and local law enforcement officials in Miami tentatively estimate that cargo theft accounts for between one-half to three-quarters of a billion dollars in lost merchandise for local shippers and freight forwarders.[20]

Since the 1970s, traditional, fixed organizational crime hierarchies have given way to entrepreneurial enterprises that are suited to specific criminal tasks. This criminal specialization allows greater flexibility, resulting in enhanced efficiency and operational effectiveness, particularly for cargo theft. Cargo thieves have proven highly adaptable, and are capable of meeting changing market needs for stolen or discounted goods.

## Cargo Fraud

Over the last two decades, fraud has increasingly become associated with organized cargo theft. Cargo fraud generally requires a high degree of sophistication and potentially generates large sums of money. Many types of fraud are effectively conducted in the freight transportation industry including:

- *Document fraud* which typically involves the sale of non-existent cargo and cargo substitution or to receive authorization from a terminal/facility to release a container.

- *Arson and insurance fraud* which occur when cargo is insured for a high value and then destroyed to obtain insurance payments.

---

[16] John Sullivan and Henry DeGeneste, Policing Transportation Facilities, Charles C. Thomas Publishing: Springfield, Illinois, 1994, pp. 28-58.
[17] Jeff Leeds, *Los Angeles Times*, "Special Report: Cargo Theft," August 10, 1997.
[18] FBI Special Agent Barry Mawn, as quoted in the *Philadelphia Inquirer* article "$38 Million in Stolen Goods Recovered," September 18, 1996.
[19] Sullivan and DeGeneste, pg. 40.
[20] John Lantigua, *The Miami Herald*, "Dade County: Hub for Hijackers and Cargo Thieves," June 12, 1997.

- *Illegal reshipment* of cargo which involves illicitly transporting hazardous wastes or strategic goods, such as weapons and weapons-grade substances, or the diversion of legitimate cargo during shipment to an alternate port or other location for illegal sale.

- *Charter fraud* which typically involves collecting freight and shipping fees from persons or parties interested in moving goods, then not chartering a carrier while keeping the fees.

## Cargo Theft: Key Findings

Changing methods for shipping high-value cargo are cited by many analysts as the major contributor to increasing cargo theft in the transportation sector. Containerization of cargo inadvertently encourages increased organized criminal presence in freight transportation. Cargo terminals, which manage the loading, unloading, storage, and transfer of these containers, are particularly vulnerable to penetration. Other key findings include the following:

- Containerized cargo theft is carried out primarily as an organized criminal conspiracy. Cargo is targeted, stolen, and fenced by criminal networks, often with the collusion of port workers, truck drivers, freight forwarders, dispatchers, and warehouse employees.

- Each year, cargo thefts from terminals (including ports, docks, intermodal facilities, rail yards, warehouses, transfer facilities), motor carriers, and maritime vessels account for between $3.5 billion (conservative FBI estimate) to more than $10 billion (NCSC estimate) in lost merchandise. This figure represents a significant portion (3.1 percent) of annual surface transportation general freight revenue.

- Indirect costs related to cargo theft (not including all law enforcement or security technology costs) range from $20 billion to $60 billion each year.

- Analysts estimate that motor carrier operations and facilities experience 85 percent of cargo theft losses. The majority of this theft occurs at cargo terminals (intermodal facilities and warehouses) that transfer or store containers from maritime vessels or rail cars to motor carriers and in local distribution facilities.

- Organized crime capabilities have expanded to allow stolen goods to first be shipped out of the United States, then shipped back into the country along convoluted routes, and then sold (as a method to legitimize illegal money, called *transshipment*). Organized crime also conducts *transnational* operations, where goods stolen in the United States are sold in other nations.

## Drug Trafficking and Money Laundering

Drugs are an international business; they are produced, marketed, finished, wholesaled, shipped, and transshipped. Transportation facilities, particularly cargo terminals, are focal points for the movement of illegal drugs, and transportation operators and security personnel play a key role in enforcing drug laws and in interdicting drugs in transit. Transportation analysts routinely cite the shipment of illegal drugs in the national transportation system as one of the most serious problems facing both the integrity and the long-term stability of the industry.

The growing volume of containerized trade provides numerous opportunities for smuggling illicit drugs. Containers sealed in one nation may not be opened until they reach a final destination in another. Both the volume of container trade and the labor-intensive methods required for inspecting containers, severely limit law enforcement personnel and freight transportation operators in identifying and preventing drug smuggling.

The Drug Enforcement Agency (DEA) reports that the use of legitimate commercial freight containers by smugglers to conceal cocaine and heroin shipments has become a large-scale problem compromising the operations of legitimate business enterprises. Victimized companies are sustaining significant financial loss, erosion of operating integrity, and diminished corporate reputation. One self-insured trucking company noted that in the second quarter of this year (1998) it had a container stolen from its facility valued at approximately $3 million.

Further, since concealment of illegal narcotics in commercial shipping is the primary method for transporting drugs and money into and out of the United States, organized crime has intensified involvement in the transportation sector. Corporations financed by drug profits may purchase, own, and operate apparently legitimate trucking companies and transportation operations to transport products and to obtain crucial shipping information. Organized criminal groups are also successfully infiltrating the transportation industry by compromising employees into acts of commission using bribery or extortion to induce collusion. In addition to transportation employees, police, customs and other government officials have been targeted for corruption.

## Drugs and Money Laundering: An Overview

The container revolution, and its importance to the U.S. freight transportation system, has paralleled the rise of the international drug trade. Illegal drug trafficking is big business:

- International trade in illegal drugs is estimated at $300 billion per year.
- Trade value is $50-$100 billion in the United States alone.
- This dollar value is second only to the global arms trade, higher than oil trade. [21]

Over the last thirty years, the United States has employed thirty-seven Federal agencies in the "war on drugs," including the DEA, the FBI, U.S. Customs, the U.S. Coast Guard, and the Secret Service. Despite record seizures and imprisonment of many traffickers over the past decade, the U.S. State Department reports that "worldwide narcotics production is reaching new levels, corruption continues to undermine enforcement efforts, and a number of governments still fail to exhibit a serious commitment to reducing drug production and trafficking."[22]

As a result of immense drug trade profits, drug trafficking groups are better organized and have more resources at their disposal than ever before. Faced with increasing governmental resistance, narcotics traffickers are relying more on indirect trafficking routes and transshipment.

In addition, drug traffickers target terminals and border checkpoints previously identified as congested and understaffed. For example, Port Newark, one of the Nation's largest sea container

[21] DEA, "National Narcotics Intelligence," 1996.
[22] Sullivan and DeGeneste, p. 90.

terminals and the fourth largest in the world, handles approximately 6,000 cargo ships carrying 1.7 million sea containers each year. Further, an estimated 200,000 containers enter this port annually by West Coast rail shipments. Of the 5,000 containers that enter Port Newark each day, Customs officials only inspect 30 to 50, accounting for approximately 1 percent of all container traffic.[23]

Cocaine comprises more than 90 percent of the drugs seized at Port Newark and has been found in a variety of sources (e.g., plastic refrigeration tubing, diesel engines, walls and ceilings of containers, concentrated fruit juices, walls of cardboard boxes, flowers, chocolates, and in plastic bags inside the stomachs of live tropical fish).[24] Additionally, one ingenious source for smuggling has been built into the base of aluminum cookware (pots/pans). Given the high volume of container traffic at Port Newark, smugglers exploit the statistically low risk of detection. Backlogged containers sit idle for extended periods of time, providing additional opportunities for surreptitious access.

In an attempt to further reduce the amount of suspected smuggling from occurring, in 1984 the U.S. Customs Service established the Carrier Initiative Program. The goal of this program is to deter narcotic smugglers from utilizing commercial air, sea, and land conveyances to transport their contraband. By signing an agreement with Customs, carriers agree to enhance their security at foreign terminals, aboard their conveyances, and at their facilities in the United States. Additionally, they agree to cooperate closely with U.S. Customs in identifying and reporting suspected smugglers. To date over 3,800 air, sea, and land carriers have voluntarily signed carrier initiative agreements with Customs. A second program was initiated in 1996. The Business Anti-Smuggling Coalition (BASC) is a business-driven and Customs-supported alliance created to combat narcotics smuggling via commercial trade. In the past three years (1995-1997) The Carrier Initiative Program, along with the Business Anti-Smuggling Coalition, have provided information to Customs which has resulted in domestic seizures totaling over 30,000 pounds of narcotics. During the same period, program participants intercepted over 70,000 pounds of narcotics destined for the United States from abroad.[25]

## Money Laundering

Commercial containerized shipments conceal money as well as illicit drugs. Currency smuggling is essential to the money laundering process, where money laundering is defined as the legitimization of proceeds from any illegal activity. Currency must be collected from local drug distributors (gangs or organizations), and then transported to specialized organized crime operations devoted to money laundering. This process is accomplished through the following steps:

1) Money is deposited into the U.S. banking system, often disguised as gambling earnings or profits from investments in other various industries.

2) Then the funds are layered through a series of mechanisms, such as wire fund transfers, designed to complicate the paper trail.

---

[23] Sullivan and DeGeneste, pp. 92-94.
[24] Sullivan and DeGeneste, pp. 92-94.
[25] U.S. Customs Service, "U.S. Customs Carrier Initiative Programs," August 1998.

3) Finally, the funds are integrated back into the legitimate economy through the purchase of properties, businesses, or other investments.

According to the U.S. Department of State's International Narcotics Control Strategy Report, the increasing concentrations of wealth among organized criminal groups is an impediment to legitimate commerce, government, and the integrity of the political process in several parts of the world.

The transportation infrastructure supports the accumulation, transportation, and legitimization of illegal profits. Both drug trafficking and cargo theft exploit vulnerabilities in the existing national transportation system. Illegal profits are made from the sale of stolen merchandise or the sale of narcotics shipped into and around the country using commercial freight transportation. Cargo theft fraud, organized crime ownership of transportation operations, and the bribery and collusion of transportation employees all serve to legitimize organized criminal activity and undermine the integrity of the freight transportation industry.

## Drug Trafficking and Money Laundering: Key Findings

Drug trafficking and money laundering are international problems that take advantage of vulnerabilities in the national transportation system:

- Each year 300 tons of cocaine enters the United States.
- High container volume and limited resources for conducting inspections result in a statistically low probability of drug detection. At most major container facilities less than 1 percent of containers can be inspected each day.
- Organized crime has invested in the transportation industry, and owns or controls its trucking companies and freight forwarders.

# 3. On-Site and Interview Findings

## On-Site Visits

On-site visits were conducted at the Port of New York/New Jersey and the Port of Boston in order to understand both crime-related problems and countermeasures and best practices in place at these locations.

### Port of New York/New Jersey

#### Description of Site

1. Kennedy International Airport and Surrounding Areas

First, as part of this study, the Port Authority police led Volpe personnel on a tour of the Port of New York/New Jersey. Activities included: a general tour of the John F. Kennedy International Airport (JFK) cargo handling areas; a tour of the state-of-the-art Japan Air Line cargo facility; overflight of the port of New York; and a tour of Springfield Gardens (an area outside of JFK populated by warehouses and cargo handling entities).

The port supports a wide diversity of business operations such as cargo storage and cargo exchange and transfer. The cargo operation at Kennedy International Airport encompasses 58 individual cargo carrier tenants. These carriers handle 197 million tons ($92 billion)[26] of cargo annually and vary widely in infrastructure and makeup. Carriers range from large companies with dedicated air cargo fleets (such as UPS), carriers moving cargo carried in the holds of major passenger liners (combination or "combi" aircraft), and cargo carried by major passenger and cargo carriers that is handled by small cargo carriers that do not operate air fleets. Each carrier is independent from the others and operates under a lease arrangement with the Port Authority. Individual facilities span from large, automated, secure, state-of-the-art facilities such as the Japan Air Line cargo terminal, to small operations consisting of an office and a single bay loading dock where all cargo is hand manipulated. Each carrier is responsible for its own security program; therefore, security at each carrier varies widely. The majority of personnel working at the major cargo terminals are employees of stevedoring firms.

The Port Authority maintains a police force with jurisdiction over all port facilities in the metropolitan area. Port Authority police have state police authority, deputy U.S. Marshall authority, and joint jurisdiction in both New York and New Jersey. The Port Authority Police *recommend* a twenty-four- (24-) point security program[27] to be followed by the tenants at all three metropolitan airports.

---

[26] Port of New York/New Jersey statistics for 1997.

[27] Caron, Robert M., Detective Lieutenant and Molina, Michael, Detective, *24 Point Security Program*, Port Authority of New York Police Department, JFK International Airport, 1997.

2. Port Newark

Second, a tour of the Port Newark container terminal was conducted. The Port Newark facility is a marine container terminal located in the southern harbor adjacent to Newark airport. Containers are typically staged at the terminal awaiting the trucker for pick-up and ultimate delivery to the consignee.

## Theft at Terminal

Although the Port Authority police maintain an active and aggressive program that addresses cargo theft, they noted that they are rarely informed of cargo theft occurrences and often information, when it is forthcoming, is not received in a timely manner. The immediate reporting of a theft, suspected theft, or any incident to cargo security personnel, company management, or law enforcement enables quick investigation and offers the best possibility for apprehension and/or recovery. Among the many reasons for lack of timely and complete information are the following:

- The vast majority of air and marine cargo transiting port facilities are not physically inspected to verify count or content. Due to the nature of cargo transportation, many losses go unnoticed until final delivery to the consignee; by that time backtracking the exact point where the loss occurred is difficult or impossible. An example was given of a leased container that returned to a U.S. port from overseas. The container was supposed to have been empty and placed in appropriate area at the facility. When the container was later opened to be loaded, it was discovered that it contained a large wooden crate. Upon further inspection the crate was found to hold a coffin containing the body of an adult male.

- Cargo theft and even sustained systematic pilferage can have detrimental impact upon the reputation of involved businesses and an entire port in general. This fact contributes to the reluctance to report any loss.

- The manner in which shipments are insured plays a role in the reluctance to report theft. Most shippers are self-insured up to certain limits; for example, one corporation interviewed identified its self-insurance limit as $500,000. Losses that fall within the self-insured limits are paid, factored into the "cost of doing business," and passed on to the consumer. To report such incidents requires employee time and, therefore, costs.

- Publicly reporting theft can have an adverse impact on the reputation of a company, facility and port, which, in turn, can affect rates charged for cargo insurance.

- Another reason for hesitancy in reporting theft is the lack of substantial outcome. Several examples were given where individuals were apprehended and prosecuted for cargo theft at an airport shipper facility. As cargo theft is usually viewed as a "victimless crime", these actions resulted in minimal fines, minimal incarceration, or dismissal.

- There is no requirement to provide police reports due to theft in order to claim the loss for tax purposes. Losses are factored into any number of accounting practices, and there is no Federal tax accounting requirement to classify cargo theft loss in such a manner that it could be retrieved for justification or data collection purposes.

- Employees, with employee cooperation or with "inside" information, perpetrate the majority of cargo theft in the Port of New York/New Jersey.

## The Port Of Boston (Massport)

### Description of Site

3. Logan International Airport

The cargo operations at Logan are conducted through eight dedicated cargo shippers with the remainder of cargo carried on board nearly thirty passenger aircraft lines that service the airport. In 1997 Logan handled 23.6 million passengers and 744 million pounds of cargo. Of the cargo handled, the majority is express small package shipments, followed by cargo shipments and mail. Of this total, approximately 190 million pounds is international cargo.[28] As with Kennedy International Airport, the physical security of the airport and access into the airport is very well controlled, making the possibility of theft perpetrated by non-employees very remote. Each cargo carrier is responsible for its own security forces, based upon FAA requirements,[29] and overall security is provided by the Port Authority. With the exception of passenger security screening personnel, all security personnel are employees of each particular shipper and not contracted. Massport's security force is made up of Massachusetts State Police officers.

4. Conley Marine Terminal

The Conley Terminal is a "rolling" container terminal (i.e., all containers awaiting shipment are mounted on trailers awaiting pick for over the road transit or delivery to the dock for loading on board a ship). As with Logan airport, access into the Conley terminal is tightly controlled.

### Theft at Terminal

The following issues were noted regarding the nature and levels of cargo-related crime at the facility:

- Similar to the findings from the New York facility, the Massport police are not advised of all instances of theft that occur. They are usually made aware as a result of direct observation or when a claim has been made to an underwriter by the shipper.

- Employees, with employee cooperation or with "inside" information perpetrate the majority of theft that does occur at Massport.

---

[28] Boston Logan International Airport Monthly Airport Traffic Summary November 1997.
[29] 14 CFR 107.

- The majority of cargo entering Conley Terminal is pre-cleared by Customs EDI procedures. Estimates of the percentage of containers actually inspected at by Customs (5 percent or less) are consistent with the GAO[30] report and the estimates received in the Port of New York and New Jersey. The average layover time for an inbound container awaiting pickup from the terminal is less than two days; however, examples were given of some cargoes being expedited (i.e., containers listed as containing "Holland tulips") so that customs processing and transport out of the terminal onto the highways can be assured within two hours of the ship's arrival at the dock. According to Massport officials, similar percentages (less than 2 percent of cargo actually inspected) are estimated for air cargo inspection. Layover time is significant in minimizing theft, which generally occurs when cargo is sitting idle.

- Domestic and international mail accounts for 143.5 million pounds of cargo shipped through Logan International Airport.[31] All mail is carried in the holds of passenger aircraft. Inbound mail is handled by the individual airlines and transported to a central U.S. Postal service terminal. As part of the Postal Service security[32] restrictions currently in place packages are limited to specific weight and size restrictions, however none of the mail is subjected to scanning. Lack of scanning is significant when considering issues such as smuggling.

## Interviews

The following issues are the result of telephone and in person interviews with state and Federal law enforcement, carrier, trade association, and terminal operations personnel. Due to the sensitive nature of the subject matter, the following information was discussed only on the condition that sources were to remain anonymous.

### Just-in-Time

Recent improvements in transportation and communication methods combined with financial pressures have resulted in the "just-in-time" concept which has reduced industry's reliance on the warehousing of stock and finished products. Today's warehouses are on rails, wheels, afloat, in the air, or awaiting transport by any of these modes. Intermodal transportation can be thought of as a "warehouse on wheels" with its own set of security needs. "Just-in-time" manufacturing increases the need for adequate security levels for shipments. Since, when utilizing such a system, there are no warehouses to backfill a stolen shipment, replacement may require weeks or months, thus amplifying the effect of a loss on the consignee.

[30] Terrorism and Drug Trafficking: Responsibilities for Developing Explosives and Narcotics Detection Technologies (Briefing Report), GAO/NSIAD-97-95, April 1997.
[31] Boston Logan International Airport Monthly Airport Traffic Summary November 1997.
[32] FAA target mail.

## Employee Screening

A common problem cited by the majority of individuals interviewed is the lack of adequate background investigations and standards for all personnel handling cargo and employed in ports and terminals. Although new FAA requirements for employee screening[33] do address specific criminal activities, other agency requirements do not, are non-existent, or are under judicial restraint. In all cases they vary by mode and are not uniform or comprehensive. Related to this issue is the lack of a uniform identification criterion and scheme. In many cases there are questionable individuals (known thieves, illegal aliens, etc.) employed in cargo handling positions.

A problem common to all ports lies in the identification and qualification of personnel employed therein and given access to port areas. There is not a standard criterion for background examination of employees for purposes of access or even for employment as a security official. Having a felony theft conviction in ones background might keep one out of specific transportation modes but it may not exclude one from employment in other facets of the transportation industry where access may be as equally critical. In many cases, mere possession of a commercial driver's license opens the gate to intermodal terminals, and organized crime entities have the capability of easily forging such credentials.

## Lack of Accountability

Several entities contacted state that the root causes of the problem of cargo theft is the lack of accountability for losses, and the minimal impact to the shipper in the event of loss. Knowing and apprehending insiders does not necessarily yield a positive outcome. Several instances were given where employees were apprehended and successfully prosecuted for cargo theft, only to receive minimal or no punishment and/or be returned to their previous positions (not all with the same shipper at a given facility but they returned to similar positions nonetheless). The reasons for this are threefold:

- Cargo theft is not in the public spotlight (regarded as a victimless crime) and therefore it does not carry severe sentencing, nor is it high on the list of criminal activity in the courts.

- Labor and civil law provisions exist that can be used to challenge port authority attempts to refuse individuals' employment based on a cargo theft conviction.

- Many organizations do not include theft as a disqualifying element of a person's record for employment purposes.

Major investigations have been conducted, some involving sting operations, and others where government and or state agents established fencing operations in order to recover merchandise and gain investigative insight. These operations recovered large quantities of high-value items

[33] 14 CFR 108.31.

(electronics, credit cards, weapons, computer components, pharmaceuticals, etc.). In all cases discussed, the majority of perpetrators arrested were employees of the facility where the theft occurred and all thefts were the result of inside operatives or information.

## Pilferage

The most common form of cargo theft is pilferage, which is most often perpetrated by employees. Figure 3 shows confiscated merchandise that reflects the ease with which large quantities of cargo can be removed from a container.

**Figure 3: Cargo Pilfered from a Container**

The practice of handlers pilfering cargo has long been an institution in the shipping industry. Manufacturers have been known to over-ship cargo to allow for the "shrinkage" that occurs due to pilferage. In the case of containerized cargo, access is achieved through the following methods:

- After offloading from the ship while the container is idle awaiting pickup/delivery in the terminal yard.
- While the cargo is undergoing consolidation or de-consolidation either at the terminal or an off-site freight forwarder.
- Anywhere along a trucking or rail route where the shipment is idle.

Instances occur in which high-value, high-technology equipment is deliberately "sidetracked" inside a carrier's terminal by employees. When it fails to arrive at the consignee, it is treated as a loss. After a period of time it legally belongs to the carrier; and, after appropriate arrangements are made between the perpetrators and associated liquidators, the shipment is sold at a fraction of its value.

The value of computer hardware and components makes such shipments an attractive target of theft. Exchanges now take place where cocaine shipments bound for the United States are traded for computer chips stolen from cargo shipments. In this scenario, both commodities have the

capacity for significant increase in value as they are passed along. Further, as an alternate method to shipping drug profits (that are in the form of cash) out of the United States, those profits are invested in stolen cargo purchased at a fraction of its value (computer hardware, memory chips, etc.) and shipped overseas as legitimate cargo, thus maximizing the capital generation of illicit activity.

One means for pilfering cargo is by removing the contents of one container and placing all or part of the contents into an adjacent container (for example, one that is empty or carrying low value cargo) that will not be monitored. Thieves have devised several ways of gaining access into shipping containers, some of which involve removal and replacement of all or part of the door hardware fasteners so that the seals and locks will not appear to have been disturbed. Once transferred, the perpetrator can arrange for removal and delivery of the stolen goods with minimal risk.

One example of the ability to remove cargo without detection is shown in Figure 4. First, a container is inspected and original seals are attached to container handles and are secured.

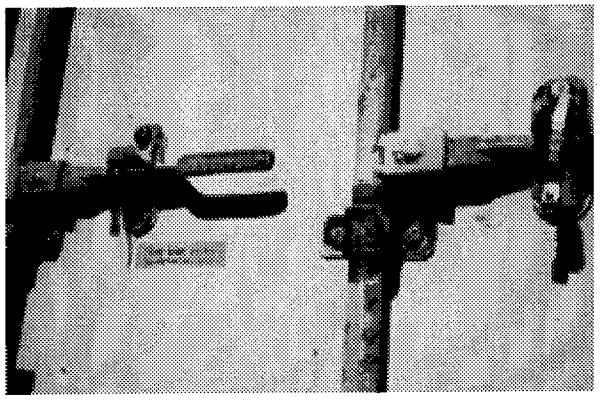


**Figure 4: Sealed Container**

Second, at some point during the shipment, a "zip" gun is used to shear the back of the rivet that attaches the handle to the guide arm mechanism, allowing the doors to be opened without disturbing the integrity of the original seals. See Figure 5.

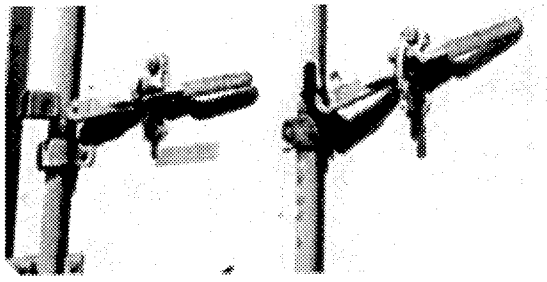


**Figure 5: Compromised Seal**

Finally, a second rivet, which was previously threaded, is then used to secure the handle and arm back together again without the appearance of having been compromised. See Figure 6.

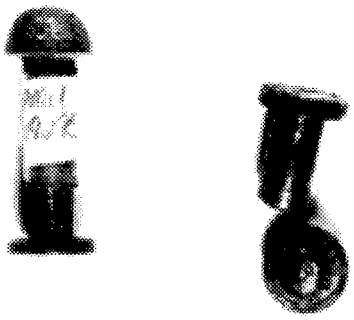


**Figure 6: Rivets**

In addition, employees of shipping companies with access to EDI applications have been able to trace shipments from point of origination to delivery at the terminal in order to arrange theft of the cargo. In some examples, current employees, using access codes that were either fabricated or belonged to other co-workers, conducted the thefts. In other cases former employees, using their old access numbers accessed shipment information via the Internet.

Deliberate misdirection of high-value cargo, to an outside, non-secured, general storage area on the tarmac or in the container yard is one method of setting up a shipment theft. Once it is misplaced, the cargo is easily transferred into other containers for delivery out of the terminal. In one instance, this cargo consisted of a large shipment of commercial grade 9mm automatic pistols. Some of those pistols were recovered by local Federal and law enforcement agencies (as shown in Figure 7). However, many of these weapons were never recovered.

**Figure 7: Recovered Weapons**

# 4. Best Practices

Cargo security is more than a function of physical security measures, it is also one of management resolve and institutional/procedural control. Regardless of the level of resolve and operational security procedures, total cargo security is impacted by the number of individual companies within a shipping route through which a shipment passes, as well as the number of institutional procedures it must pass. As each company has its own procedures, the security of a shipment subjected to several modes during a transit is inversely enhanced according to the number of hands it must pass. The more uniform the security controls and accountability are, the greater the level of transit integrity. "Exclusive" shippers, i.e., those who own and operate the entire route from start to finish generally suffer the least amount of security breaches and loss from outside sources. The degree of loss and risk increases as more entities are given access and control of shipments.

Based on this study, carriers who place the most management emphasis on security have the most successful security programs. These carriers tend to have established standards for all contract carriers; subject those carriers to periodic audits to ensure standards compliance; and rely on strict contractual arrangements. Provisions of a similar nature are being enacted by a consortium of American computer manufacturers known as Technology Asset Protection Association (TAPA), in an attempt to standardize security procedures and enforce liability with specific regard to facilities that handle its shipments (see Appendix C).

Further discussion leads to the approach for implementing the industry provided Best Practices and each category is explained below, with examples of best practices from various providers, and the U.S. Customs Service.

## Policy, Procedures, and Guidelines

Research for this first phase of "best practices" identification indicates that each participant in the transportation of cargo is actively engaging in practices that are designed to maintain, or in some cases increase, the integrity of security systems while achieving increased security of the cargo in transit. Successful preparedness ensures the selection of optimal policies and procedures, their documentation in clear and widely distributed plans, their integration into Standard Operating Procedures (SOPs) wherever possible, and their effective implementation through comprehensive and effective training programs and drills. These programs have been shown to be quite effective as demonstrated by the Port of New York/New Jersey's "24 Point Security Program".

### Industry Recommendations

1. Conduct a program of periodic security seminars for all employees involved in cargo handling and documentation processing, stressing the importance of the following:

    - Maintaining legible and accurate cargo tallies.

    - Processing only legible documents.

- Writing only in ink or ballpoint pen.
- Completing all information required by shipping documents.
- Obtaining clearly written signatures.
- Safeguarding the confidentiality of shipping and entry documents.
- Maintaining good cargo security generally.

2. Include posters, stickers, payroll stuffers, monetary incentives, and properly worded reward signs in the security awareness program.

## Collection and Dissemination of Data

The first step in reducing the problem of cargo crime at terminals is the assessment of the size and nature of the problem or, in other words, the collection of data. One industry attempt to collect and disseminate cargo theft data is the TIPS II database system, a creation of the Transportation Loss Prevention and Security Council of the American Trucking Association (ATA). In addition, some state and local law enforcement agencies have developed systems to compile cargo security data for their region. Cargo TIPS II is a secure Internet system that consists of the following major components:

- Cargo Theft Report – Allows entering, editing, and updating of theft reports
- Reports and research – Unlimited database research
- U.S. Customs theft reports by commodity, location, time period, etc.
- Hot Sheet – Bulletin board/E-mail alert system

Also critical to reducing crime is the dissemination of information, which allows carriers and others to take actions with the goal of strategically reducing losses. Insurers are taking an active role in working to reduce losses. For example, CIGNA Insurance Companies provides CIGNA Ports of the World, a guide to aid traders and shippers. The guide includes current port conditions, guidelines for assure secure cargo transportation, and recommendations to minimize cargo loss and damage. In addition, the Port of New York/New Jersey Police have implemented a 24 Point Security Program, which provides guidelines for a series of best practices and a security awareness program known as "Crime Watch," which affords employees the ability to report crimes and receive a monetary reward.

### Industry Recommendations

1. Develop a comprehensive system for the accurate collection of cargo theft data.

2. Provide shippers with up-to-date information.

## Coordination and Cooperation

Several terminals studied have developed cooperative entities and programs to address specific crime issues. For example, in response to extensive problems with organized crime in the New York/New Jersey port district, the Waterfront Commission of New York Harbor was established in 1953. Today, the Waterfront Commission has broad investigative, licensing, regulatory, and police authority over piers and terminals in the port district. It investigates criminal activity, registers and licenses longshoremen, stevedore companies, hiring agents, pier superintendents and pier guards, regulates and monitors dock employment, and exercises broad police authority.[34]

Multidisciplinary programs are in use at some terminals to target cargo crime. These programs like "Operation Kat-Net", involved New York's Port Authority Police, regional police organizations, FBI, and the states District Attorney's Office and focused on reducing cargo crime in targeted high-theft areas. Several other undercover operations were implemented to reduce incidents of crime. Operation conducted by the FBI's San Jose-based high-tech crime squad — Operation "Dragon Teeth" in 1994, Operation "Chiptryster" in 1995, Operation "Westchips" in February, 1996 and Operation "Bytes Dust" in April, 1996 have put a significant dent in premises thefts, particularly in California. Those arrested in these roundups have also been linked to home invasions, money laundering and counterfeiting activities, illegal gambling, fictitious business frauds, as well as a myriad of drug and weapons violations.[35]

### Industry Recommendations

1. Use regional multijurisdictional entities focused on reducing crime.

2. Implement multidisciplinary cargo theft task force programs.

3. Design undercover law enforcement operations directed at specific problem areas.

## Personnel Issues

### Employee and Independent Contractor Background Checks

Operators of cargo handling facilities should conduct employment screening of prospective employees. (Customs Regulations, already require international carriers, proprietors of bonded warehouses, and customhouse brokers to submit employee lists upon request from the district

---

[34] Policing Transportation Facilities, p. 34.

[35] "High Tech Cargo Theft", A Presentation at the U.S. Capitol, MaryLu Korkuch, Executive Director, Technology Theft Prevention Foundation, April 9, 1996.

Director of Customs. Such lists should contain the name, address, social security number, and date and place of birth of each employee and be kept up to date.) For example, the Waterfront Commission of New York Harbor actively monitors port employment, providing licenses for longshoremen, checkers, hiring agents, pier superintendents, pier guards, stevedore companies, and telecommunication systems controllers.[36]

## Industry Recommendations

1. Require all personnel, including maintenance and clerical personnel, who will have access to cargo areas and shipment-related documentation to submit a detailed employment application, which contains a photograph of the applicant, a list of past residences, and a prior employment history for the preceding 10 years.

2. Screen all such applicants for the following:

   - Verification of address and prior employment,
   - Credit record, and
   - Criminal record, if possible.

3. The background and corporate structure of independent contractors providing janitorial service, refuse disposal, or other service should be verified. Access by independent contractors to the facility should be under security controls by performing the following activities:

   - Periodically examine independent contractor vehicles, which are parked in or near cargo areas.
   - Permit independent contractor employees to enter only those areas necessary for their particular work; permit them access to cargo areas and areas where shipping documents are located only under the supervision of security and/or management personnel.
   - Require independent contractors to display identification similar to that required by the facility for its own employees.

## Security Staff

Operators of cargo handling facilities should employ a Security Officer or assign a particular officer of the firm to be responsible for security. All operators handling a substantial volume of international cargo should provide guards to protect the cargo.

[36] Policing Transportation Facilities, p. 35.

## Industry Recommendations

1. Employ a number of guards adequate to provide appropriate security for the size of each facility and the volume of cargo handled. Alarm systems, closed-circuit television, and other security devices may reduce the number of guards needed.

2. Train all company employee guard forces or ensure that contract guard forces are trained in the following:

   - Methods of patrolling terminals and warehouses
   - Use of firearms and other equipment that may be furnished
   - Report writing, log and record keeping
   - Identification of security problems and specific trouble areas

   The security manager should appoint a person to be in charge of the training function. But beware: Appointing a trainer who does not quite understand the security function could seriously compromise the effectiveness of the security program.[37]

3. Equip the guard forces with uniforms that are complete, distinctive, and authoritative in appearance.

4. Provide firearms, vehicles, communications systems, and other equipment deemed necessary for the successful performance of the guard function.

5. Insist on physical fitness as a prime consideration in selecting a guard force. Require guards to undergo self-defense training similar to that of police agencies. Require a physical examination at least once a year.

6. Furnish each guard with a manual covering operating procedures and standards of conduct, and clear statement of what management expects.

7. Ensure adequate and reliable communications between elements of the terminal security force and from the security force to local police.

8. Provide security personnel with a telephone at fixed posts or two-way radio, intercom, duress signal communication, or other type of equipment providing voice communication capability within the company.

9. Arrange assured means (telephone, radio, or special alarm line) for summoning assistance from local forces.

---

[37] Gomez, Herman, Captain, "The Importance of Maritime Security Training Worldwide," Maritime Security Manual, American Society for Industrial Security, 1990.

10. Provide training on appropriate cargo handling and loading procedures as well as appropriate cargo documentation handling.

## Identification System

All operators of facilities handling a substantial volume of cargo should employ an identification card system to identify personnel authorized to enter cargo and document processing areas. If a facility is not implementing an access control system for authorized entry, then, at a minimum, an identification card system should be implemented.

### Industry Recommendations

1. Include the following information on the ID card: (a) physical description or, preferably, a color photograph of the holder, (b) name and address, (c) date of birth, (d) employer's license number, if any, (e) signature of holder, and (f) reasonable expiration date.

2. Laminate all cards to prevent alterations

3. Assign each card a control number.

4. Recover ID cards from terminated employees.

5. Require each employee to display his or her ID card to gain access to the facility, to cargo areas within the facility, and to areas where shipping document are processed. Preferably, the ID card should be displayed so that it is visible at all times that the employee is within the facility.

## Facility Access Control Measures

Many transportation companies, ports, or port facilities have taken steps to reduce system vulnerability to acts of theft by using various access control measures. All cargo handling and storage facilities should provide a physical barrier against unauthorized access to cargo. Usually this requires a covered structure with walls that can be securely closed and locked.

Some access control equipment, such as gates, is extremely straightforward. Some facilities, however, employ more sophisticated technology such as the following:

- Intrusion-detection alarms: Electromechanical, microwave, infrared, dual technology, and acoustic.

- Access control: Electronic access control systems, magnetic-card key; employee sign-in procedures, work order procedures, fences and gates, locks, vaults.

- Communications: Radio, public address system, emergency station and rail car phones, train annunciator systems, silent alarms.

- Vehicle barriers: Concrete barriers for placement to protect system.

Over the last decade, electronic Access Control Systems (ACS) technology has improved significantly in efficiency and reliability. Recent innovations include:

- Improvements in off-the-shelf distribution database software.
- The introduction of the micro controller (enables fault tolerance and independent decision making for access denial and alarm triggers).
- The development of miniature micro-controllers that can be housed in the card reader panel and do not require separate wall panels and wiring.

In addition, CCTV and "smart" building management systems have revolutionized ACS capabilities. Software innovations allow electronic ACS technologies to be integrated with Building Management Systems, Fire Detection and Suppression Systems, and CCTV Surveillance Systems. There are various basic electronic ACS devices:

- Card Readers
- Alphanumeric Code Entry Systems
- Personal Feature Identification (PFI)/Biometric Systems[38]
- Remote Terminal Unit or Local Controller
- File Server or Computer Work Station

## Fencing

Fencing may be needed:

- As supplementary protection to prevent unauthorized persons and vehicles from entering cargo storage and handling areas, and
- As sole protection for open storage of bulk cargo or large articles which do not require covered storage because they cannot be easily pilfered or removed without mechanical handling equipment or which have their own inherent security (containers).

Where fencing is required, it should enclose an area around cargo storage structures, support buildings, and exterior stored cargo sufficient to provide maneuvering space for pick-up and delivery vehicles and to prevent use of buildings or cargo to go over fences. The fence line must be inspected regularly for integrity and any damage promptly repaired.

### Industry Recommendations

1. Install chain-link fencing, at least 9 gauge, 2-inch mesh, and at least 8 feet high (not including a barbed wire outrigger). If the level on which the fence is constructed is lower than the area

[38] Boyd, M. Annabelle and Maier, M. Patricia. *State Safety Oversight Security Handbook*, USDOT, FTA, 1997.

outside the fence line, increase the height of the fence to provide an effective 8-foot fence at all points.

2. Top the fence with a 2-foot barbed wire outrigger, consisting of double-twisted barbed wire, properly spaced and at a 45-degree angle to the vertical.

3. Utilize tensioned wire on *top* of fence fabric in lieu of rigid top rail. Bottom of fence may utilize rigid rail for securing fence fabric to posts.

4. Place fence posts inside of the fence and secure them in a cement foundation at least 2 feet deep.

5. If warranted, install a kinetic energy barrier (heavy-grade, tensioned cable secured off the fence to prevent vehicle penetration of fence line)[39]

6. Ensure that objects or persons cannot pass beneath the fencing by providing:

   - Cement aprons not less than 6 inches thick
   - Frame piping
   - U-shaped stakes driven approximately 2 feet into the ground

7. Avoid any condition that compromises the fence line. Prohibit the placing of containers, dunnage, cargo, vehicles, or any other item that may facilitate unlawful entry adjacent to the fence line. Where necessary, install bumpers or fence guards to prevent damage by vehicles.

## Gates

Gates provide access for both legitimate and illegal activities. As such, they must be designed into the facility appropriately and monitored on an ongoing basis to achieve an appropriate security level.

### Industry Recommendations

1. Reduce the number of gates in fences to the minimum necessary for access.

2. Ensure that all fence gates are at least as substantial as the fence.

3. Gates through which vehicles or personnel enter or exit should be continuously manned or under observation by management or security personnel.

4. Equip gate with a deadlock bolt or substantially equivalent lock that does not require use of a chain. All hardware connecting the lock to the gate should be strong enough to withstand constant use and attempt to defeat the locking device.

---

[39] The Making of a High Security System, A Presentation at American Defense Preparedness Association, Robert F, Hoaglund CPP, 1990.

5. Construct swing-type gates so that they may be secured to the ground when closed.

6. Separate gates for personnel and vehicle traffic are desirable.

## Doors and Windows

All buildings used to house cargo and associated support buildings should be constructed of materials that resist unlawful entry. The integrity of the structure must be maintained by periodic inspection and repair. Security protection should be provided for all doors and windows.

### Industry Recommendations

1. Equip all exterior doors and windows with locks.

2. Protect all windows through which entry can be made from ground level by safety glass, wire mesh, or bars.

3. Similarly safeguard all glassed-in areas where shipping documents are processed.

4. Construct all delivery and receiving doors of steel or other material that will prevent or deter unlawful entry. Keep these doors closed and locked when not in use.

5. Where fencing is impractical or guards insufficient, equip the building with an intrusion detection or alarm system.

6. Ensure that there are no avenues for surreptitious entry through floors, roofs, or adjacent buildings.

7. Equip emergency exits with intrusion alarms. These alarms are equipped with audio alarms, flashing lights, and a verbal annunciator that warns intruders of their unauthorized entry. The alarms are connected, via dedicated lines, to alarms and printers in a secured location.[40]

## Locks and Key Control

Locks or locking devices used on buildings, gates, and equipment should be so constructed as to provide positive protection against unauthorized entry. Management or security personnel should control the issuance of all locks and keys.

### Industry Recommendations

1. Use locks having (a) multiple pin tumblers, (b) deadlocking bolts, (c) interchangeable cores, and (d) serial numbers.

---

[40] Donohue, Kenneth J. *Terrorism: Real Life Experiences, The American Perspective*, FTA, 1996.

2. To facilitate detection of unauthorized locks, use only locks of standard manufacture displaying the owner's company name.

3. Number all keys and obtain a signature from the recipient when issued. Maintain a control file for all keys. Restrict the distribution of master keys to persons whose responsibilities require them to have one.

4. Safeguard all unissued or duplicate keys.

5. Remove and secure keys from cargo handling equipment and vehicles when not in use.

## Automated Gatehouse Facilities

Automated gatehouse facilities use information systems to match cargo, paperwork, trucks, and drivers at exit points, and are designed to reduce the illegal movement of goods out of facilities. The Seagirt Marine Terminal at the Port of Baltimore uses a computerized gate complex that serves as the nerve center for the terminal. Seagirt's automated system consolidates the steps necessary to generate the Trailer Interchange Report (TIR). When trucks enter the terminal, an electronic sign-bridge over 13 of the 14 inbound lanes directs the drivers to the appropriate lane, where a remote intercom system serves to quickly exchange information with clerks in the gatehouse. For export traffic, trucks are directed to one of four lanes with built-in scales. While the driver supplies the clerk with the necessary information, the container's weight is automatically input into the clerk's computer. The driver then pulls under the gatehouse canopy, where a terminal mechanic inspects the container and chassis for any damage. Should any be found, the Seagirt computer prohibits the clerk from reassigning the equipment until it has been repaired. The driver then receives the TIR and is released into the terminal. The process for import loads is essentially the same. The clerk verifies the driver's information and that the container has received all the appropriate releases. The clerk then issues the TIR, informing the driver where the container is stored. After picking up the container, the driver goes to one of the five outbound lanes, where a security check and final inspection are performed.[41]

Operators of facilities handling a substantial volume of cargo should maintain a manned gatehouse at all vehicle entrances and exits during business hours.

### Industry Recommendations

1. Set the gatehouse back from the gate so that vehicles can be stopped and examined on terminal property.

2. Equip the gatehouse with a telephone, duress, or other communication system.

3. Clear the area around the gatehouse of any encumbrances that restrict the guard's line of vision.

[41] Port of Baltimore Web site, http://www.mpa.state.md.us/.

4. Post prominently on the exterior of all gatehouses signs advising drivers and visitors of the conditions of entry. Include in conditions of entry a notice that all vehicles and personnel entering the area are subject to search.

5. Provide equipment and employ processes to thoroughly verify documents presented by drivers.

## Parking Areas

Private passenger vehicles should be prohibited from parking in cargo areas or immediately adjacent to cargo storage buildings. Access to employee parking areas should be subject to security controls.

### Industry Recommendations

1. Locate parking areas outside of fenced operational areas, or at least a substantial distance from cargo handling and storage areas or buildings and support buildings.

2. Require employees exiting to the parking area from the cargo area to pass through an area under supervision of management or security personnel. Require employees desiring to return to their private vehicles during hours of employment to notify management and/or security personnel.

3. Allow parking in employee parking areas by permit only. Maintain a record of each issued permit, listing the vehicle registration number, model, color, and year. The permit should consist of a numbered decal, tag, sticker, or sign placed in a uniform location on the vehicle.

4. Issue to vendors and other visitors temporary parking permits which allow parking in a designated area under security controls.

## Lighting

Lighting is a valuable, and generally inexpensive, method of increasing security levels at facilities.

### Industry Recommendations

1. Illuminate all vehicle pedestrian gates, perimeter fence lines, and other outer areas with mercury vapor, sodium vapor, power quartz lamps, or substantially similar high intensity lighting, employing a minimum of 400 watts per fixture. The Society of Illuminating Engineers recommends the following light intensities measured at ground level.

    - Vehicle and pedestrian areas — 2.0 foot-candles
    - Vital structures and other sensitive areas — 2.0 foot-candles
    - Unattended outdoor parking areas — 1.0 foot-candle

2. Protect lighting subject to vandalism by wire screening or other substantially equivalent means and establish a system of planned maintenance. When installing, locate lights 30 feet above ground level and properly spaced to provide the appropriate light intensity for the area to be illuminated. Adequate lighting should be provided for the following areas:

   - Entrances, exits, and around gatehouses.
   - Cargo areas, including container, trailer, aircraft, and rail-car holding areas.
   - Along fence lines and parking areas.

## Monitoring and Tracking

### Closed-Circuit Television

The use of closed-circuit television (CCTV) has become increasingly popular in the security industry. CCTV can be used for real-time monitoring and/or video recording, thus providing terminal users a means by which they could view system operations and suspicious activities. The reasons behind employing CCTV technology may vary from location to location, but several applications are generally consistent with this form of surveillance technology (see Table 1).

**Table 1: CCTV Technology**

| Application | Description |
|---|---|
| **Monitoring of Facilities** | Use of CCTV to view yards/docks/terminals. Camera feeds may be directed to a centralized location or to a localized monitoring area (e.g., Security Booth or office) |
| **Incident Management** | Camera feeds to central control to enable personnel monitoring CCTV to call staff to respond to an incident; to enhance accurate description of incident; to provide a video record with time/date stamp |
| **Legal Evidence** | Continuous, random, or emergency monitoring of facilities or vehicles for use as evidence in legal proceedings |
| **Security of Problem Areas** | Use of CCTV in difficult-to-patrol areas such as parking lots to deter criminal activity; to support police operations; to enhance incident response |
| **Special Police Operations** | Portable or mounted cameras used to assist undercover police officers in observing facilities; identifying perpetrators; documenting activities |
| **Risk Management** | Verification of insurance claims against the company, typically resulting from (alleged) accidents |

One facility contacted during the course of this study is installing a fiber optic CCTV system. This technology will utilize a distribution system that connects all CCTV cameras through a Local Area Network (LAN) so that any location on the LAN can access real-time video from any camera on the network. Signals are transmitted to the LAN over fiber optic cables. This system will be connected directly to a Central Control, with feeds available at the local areas as well. This CCTV surveillance system will allow a dispatcher at a remote console to assess a given

situation and dispatch the appropriate personnel to any incident. Videotape can also be recorded off any camera on the LAN.

## Use of Secure Areas

Adequate space capable of being locked, sealed, or otherwise secured for storage of high-value cargo and packages which should have been broken down prior to or during the course of unloading must be provided at each cargo handling building. When such cargo must be transported a substantial distance from the point of unloading to the special security area, vehicles capable of being locked or otherwise secured must be used. (These standards are required by Customs Regulations, 19 CFR 4.30.)

### Industry Recommendations

1. Construct special security rooms, cribs or vaults so as to resist forcible entry on all sides and from underneath and overhead.

2. Locate such special security areas, where possible, so that management and/or security personnel may keep them under continuous observation. Otherwise, install an alarm system or provide for inspection at frequent intervals.

3. Release merchandise from such an area only in the presence of authorized supervisors and/or security personnel.

4. Log all movements of cargo in or out of a special security area, showing date, time, condition of cargo upon receipt, name of truckman and company making a pick-up, and registration number of equipment used.

5. Perform a physical inventory of secure areas every eight hours or every shift. Maintain a logbook that itemizes all shipments entered and removed. Two separate locks and keys to the secure area can be used with different individuals, one being management, and having access to each of the keys.

## Advanced Computer Systems/Software to Monitor and Track Shipments

The Ports of Seattle and Tacoma use an electronic data interchange (EDI) system called LINX to optimize movement of goods through the port. The Port of New York and New Jersey uses the Advanced Cargo Expediting System (ACES) to provide shipment status and location information. Information provided includes arrival notices from ocean carriers, delivery orders from customs house brokers, cargo status replies from marine terminals, and electronic bookings from freight forwarders to ocean carriers.[42]

[42] Intermodal Freight Transportation, 3rd Edition, Gerhardt Muller, p. 190.

### Industry Recommendations

1. Use EDI systems to optimize movement of goods through the port.

2. Use computer systems to provide shipment status and location information.

## Automatic Equipment Identification Technology

Several carriers have begun to use Automatic Equipment Identification (AEI) technology that relies on bar codes and bar code scanners with radios to transfer real-time data on shipping containers and vehicles. Benefits include accurate data entry, faster location of containers in terminals, and reduced workforce requirements.[43]

### Industry Recommendations

Use AEI technology to transfer real-time data regarding the following:

- Shipping container and/or vehicle locations
- Container identification
- Chassis management
- Automatic container/trailer weighing
- Gate access control
- Intermodal movement operations

## Global Positioning Systems

Many companies currently use Global Positioning Systems (GPS) to track the worldwide movement of their ships and provide customers with accurate status and arrival information. GPS technology may be used (in combination with other technologies such as AEI) to track the movement of individual containers from the time they are loaded until they reach their final destination.

### Industry Recommendations

1. Implement GPS to track shipment status.

2. Use GPS in combination with other tracking technologies.

[43] Intermodal Freight Transportation, 3rd Edition, Gerhardt Muller, p. 192.

## Tracking of Goods to Prevent Theft

All of these technologies provide some capability in pinpointing the location of goods at each step in their movement from origin to destination. Finding the location at which the subversive activity is occurring is paramount in order to focus the required security resources appropriately. Gate passes should be issued to truckmen and other onward carriers to control and identify those authorized to enter the facility. Verification of the identity and authority of the carrier requesting delivery of cargo should be made prior to the cargo's release.

### Industry Recommendations

1. Require truckmen to submit proper identification (such as a driver's license or USCG Port security ID card) and a vehicle registration certificate before being issued a gate pass and being permitted to enter the facility; require them to surrender the gate pass before leaving the facility.

2. Seal containers and trailers and note the seal number on the gate pass before delivery is effected. Verify the seal number when the gate pass is surrendered at the gate.

3. Require the company name of all onward carriers to be clearly shown on all equipment. Do not accept temporary placards or cardboard signs as proper identification of equipment. Require carriers using leased equipment to submit the lease agreement for inspection and note the leasing company's name in the delivery order.

4. Release cargo only to the carrier specified in the delivery order unless a release authorizing delivery to another carrier, signed by the original carrier, is presented and verified. Accept only original copies of the delivery or pick-up orders.

5. Personnel processing preloaded delivery or pick-up orders should verify the identity of the truckmen and the trucking company before releasing the pick-up order. Limit access to areas where such documentation is processed or held to authorized personnel and rigorously safeguard all shipping documents from theft or unauthorized observation.

6. Conduct delivery and receiving operations at separate docks or doors, if feasible.

## Container Seal Improvements

High-value containerized cargo is being secured with bolt or cable barrier locking systems, which tie a container's two central locking bars in such a way that even if a barrier seal on the handle is removed, or the handle itself is detached from the lock rod, it is impossible to open the doors in the normal manner. Carriers are obligated to seal all containers entering the United States with a high-security bolt red seal. This applies whether or not the container is empty of loaded. A high-security bolt blue seal is used for all containers being exported out of the United States. Control and disposition of seals is vital and specific records or logs must be kept. There are several such products available. Models use either a reusable pick- and-drill-resistant locking cylinder or a single-use disposable unit, suitable for areas where recovery of reusable locks is difficult.

Container seal tape that changes color or appearance when opened also makes theft or tampering more difficult to conceal. Furthermore, in order to reduce losses, insurance companies and shippers are now pressuring shipping lines to secure containers with heavy-duty barrier seals, even to the extent of making this a condition of insurance.[44]

All containers, trailers, rail cars, and air cargo lockers entering or leaving a facility should be sealed. Mounted and high-value containerized shipments should receive special security attention.

## Industry Recommendations

1. Inspect seals whenever a sealed containerized shipment enters or leaves a facility. If the seals are not intact or there is evidence of tampering or the seal numbers are incorrect, notify security and/or management personnel and tally the cargo.

2. Seal unsealed containerized shipments at the point of entry to the facility and note the seal number on the shipping documents. Seal all containerized shipments leaving the facility and note the seal number on the shipping documents. Inspect the contents of containers received in an unsealed condition.

3. Release seals to as few persons as possible. Require all persons handling seals to maintain a strict control of the seals assigned and to store them in a secure place.

4. Maintain a seal distribution log, which indicates to whom seals have been released.

5. Where possible, secure containers by butting or "marrying" their door ends against each other. However, do not butt them against a perimeter fence or building wall if that will compromise the protection provided by the fence or wall. In stacking containers, place those containing high value merchandise on top. Finally, containers or trailers can be backed up tightly against a loading bay door to protect from thieves who do not have access to the warehouse.

6. Locate high-value merchandise in mounted containers or trailers in a special security holding area where it can be observed by management and/or security personnel.

7. When containers are mounted on chassis, secure fifth-wheel by a pin-lock which meets the minimum standards for locks and is constructed to withstand normal abuse from equipment. Hold designated management and/or security personnel responsible for storage and control of pin-locks.

8. Restrict access to special security holding areas and permit the release of containers or trailer from such areas only in the presence of management representatives and/or security personnel.

---

[44] "Fraud, Hijacking and Theft of Valuables," Patrick Barco, Chair, Container Security, Canadian Bureau of Marine Underwriters, www.webcom.com/cbmu.

9. Record movements of containers in or out of a special security holding area, showing: date, time, seal number, name of truckman and company making pick-up, and registration number of equipment used.

## Information Technology Systems (ITS) Security

To address vulnerabilities of data that are critical to the security and integrity of ITS systems, a variety of methods, such as access control to centralized computer facilities and computer security measures (firewalls), are used. Also, routine backups of data and redundant (backup) computer hardware further protect these systems.

### Industry Recommendations

There are numerous actions that can be taken when designing or purchasing an information technology system to provide enhanced security. Detailed recommendations regarding system configuration are included in Appendix B.

# 5. Conclusions and Countermeasures

- The lack of definitive cargo loss and theft data necessary to establish the scope and extent of security weaknesses is disturbing and denies transportation, public safety, and security professionals a very important tool in the prevention of unlawful activity. Locations of where cargo is compromised remains elusive; as well as the amount and frequency at which cargo theft or diversion occurs. This situation makes the development and implementation of countermeasures all the more difficult. Efforts to collect and analyze this data must be instituted, preferably through government-industry cooperative efforts. At this time, a good first step is one of industry's attempt to collect and disseminate cargo theft data throughout the shipping and law enforcement communities identified as the TIPS II database system, a creation of the Transportation Loss Prevention and Security Council of the American Trucking Association. This system is currently in use by major highway shipping companies as well as Federal, state, and local law enforcement.

- The diversity in cargo physical/information security topics and overall business architecture demonstrates the need for a systemwide analysis of cargo security. This analysis should not only address physical and procedural security, but address the business and legal infrastructures which impact upon security (such as taxation, insurance, anti-trust, organized labor, and organized crime concerns). The systemwide analysis and risk assessment of cargo security would have to include analysis of physical security plans and standard operation procedures in the cargo transportation community to address potential threats by considering the following elements:

    1. Electronic Data Interchange (EDI)
    2. Perimeter (fencelines, entrances/access points, docks, mooring)
    3. Cargo container vulnerabilities
    4. Cargo Storage (high value commodities)
    5. Seal Accountability
    6. Internal Accountability

- Further study should be made into the international trade routes from which cargo shipments originate. It is recommended that further government efforts focus on methods of verifying EDI networks and shipping methods at foreign locations and validating cargo prior to shipment into the United States. The security of both the item shipped (seals, alarms, tracking, locks) and access to that item internationally and nationwide (identification, background investigations, etc.) with the goal of creating uniform guidelines, requirements, or standards.

- Joint Federal and industry efforts should be undertaken to standardize cargo security requirements. Examples of issues for possible exploration are: establishment of a uniform personnel background investigation requirement and the related establishment of a nationwide scheme for personnel access and identification.

- In order to provide a platform for demonstration of security concerns across intermodal transportation, and to foster political support for improvements in transportation physical

and information security, a series of "test beds" should be established in selected ports and facilities. The results of these demonstrations will be used as case studies to greatly assist in the identification of the scope and extent of cargo loss, allow for prioritization of equipment and procedures to recommend and surface possible remedies to augment security guidelines.

- Furthermore, programs of all Federal Government agencies exercising authority over programs, which effect cargo and shipping, should be analyzed. The resultant objective will be the creation of a cargo security program that integrates Federal requirements with commercial industry best practices and may be used as a benchmark in the industry by which all could use to enhance safety and security. One such initiative that the Port of New York/New Jersey has implemented is an employee program known as "Crime Watch". This program has been very successful in providing law enforcement with crucial information regarding cargo theft and other violations.

- Technology improvements in the areas of non-intrusive cargo screening and cargo intrusion/tracking need to be evaluated for specific applicability to the interests of contraband detection, and suppression of criminal/terrorist use of the transportation infrastructure. Further, coordinated development of non-intrusive cargo inspection, cargo tracking, and cargo intrusion detection systems will be helpful in preventing duplication of government efforts, but more importantly will aid in the detection of specific points in shipment where loss/tampering occurs.

# Appendix A: Intermodal Cargo Security Study

**Name:**_____
**Title:**_____
**Company:**_____
**Phone:**_____
**Fax:**_____

## 1. PROFILE

A. What are the primary cargo types handled by your company?

| | |
|---|---|
| Dry Bulk | _____ |
| Liquid Bulk | _____ |
| Container | _____ |
| Roll on Roll off | _____ |
| Non-Containerized General (including breakbulk) | _____ |

| B. Cargo documentation | Y | N |
|---|---|---|
| Does your company handle military cargo? | _____ | _____ |
| Does your company act as forwarding agent for cargo carried ? | _____ | _____ |
| Does your company transport cargo processed by other entities? (freight forwarding agents, government entities) | _____ | _____ |
| Does your company transport cargo originating in other modes? | _____ | _____ |
| Does your company transport cargo originating from abroad? | _____ | _____ |
| Does your company use electronic procedures for: | | |
| Cargo booking | _____ | _____ |
| Manifests | _____ | _____ |
| Customs processing | _____ | _____ |
| Cargo tracking | _____ | _____ |

C. Do you conduct cargo verification inspections to identify the actual cargo carried and state of cargo carried? _____ _____
If yes, explain how.

D. If cargo verification inspections are conducted, on what basis are they held?

| | | |
|---|---|---|
| Routine (state frequency) _____ | _____ | _____ |
| At customer request | _____ | _____ |
| At the request of law enforcement entities | _____ | _____ |
| Upon receipt of alert to criminal/terrorist activity | _____ | _____ |

## 2. SECURITY FORCE AND TRAINING

| | Y | N |
|---|---|---|
| A. Does the company have a designated security officer? | _____ | _____ |
| B. Does each facility/division have a dedicated security force? | _____ | _____ |
| C. Is training provided to the security force? | _____ | _____ |

D. If yes, what topics are covered in security force training?

| | | |
|---|---|---|
| Federal security procedures (DOD 5225.22M , etc.) | _____ | _____ |
| U.S. Customs requirements | _____ | _____ |
| Immigration and Naturalization Service requirements | _____ | _____ |
| State Department requirements | _____ | _____ |
| State procedures (including port authority) | _____ | _____ |
| Local police procedures | _____ | _____ |
| Company procedures | _____ | _____ |
| Hazardous Materials Transport | _____ | _____ |
| Hazardous Materials Response | _____ | _____ |
| First aid | _____ | _____ |
| Self defense | _____ | _____ |
| Use of force | _____ | _____ |
| Weapons use | _____ | _____ |
| Explosives, Nuclear, Biological, Chemical agent response. | _____ | _____ |
| Terrorism response procedures | _____ | _____ |
| Labor unrest | _____ | _____ |

Other

_____

_____

_____

E. Are standard procedures in effect dealing with

| | | |
|---|---|---|
| Federal security procedures (DOD, Customs, INS, FBI) | _____ | _____ |
| State procedures | _____ | _____ |
| Local police | _____ | _____ |
| Company security procedures | _____ | _____ |
| Hazardous Materials Transport | _____ | _____ |
| Hazardous Materials Response | _____ | _____ |
| First Aid | _____ | _____ |
| Self defense | _____ | _____ |
| Use of force | _____ | _____ |
| Explosives, Nuclear, Biological, Chemical agent response. | _____ | _____ |
| Terrorism response procedures | _____ | _____ |
| Labor unrest | _____ | _____ |

Other _____

## 3. FACILITY SECURITY

A. By what means are secure/restricted areas established for:

Warehousing/staging of cargo _____
Inspection of cargo _____
Inspection of vehicles _____
Inspection of personnel _____

| | Y | N |
|---|---|---|

B. Does the facility have a secure communications system between:

| | | |
|---|---|---|
| Patrol units and the security control area | _____ | _____ |
| Security control to local police | _____ | _____ |
| Security control to state police | _____ | _____ |
| Security control to federal law enforcement authorities | _____ | _____ |

C. What forms of identification are required for access onto/into:

Warehouses _____
Port facilities _____
Tank farms _____
Freight yards _____
Vessels (moored at facility) _____
Vessels (elsewhere) _____
Containers (on shore facility) _____
Containers (on board vessel) _____
Containers (on board highway trailer) _____
Trucks (within facility) _____
Trucks (outside facility) _____
Pipelines (within facility) _____
Pipelines (outside of facility) _____
Trailers _____

| D. Does your company/facility participate in or conduct drills for the following contingencies on a regular basis: | Y | N |
|---|---|---|
| Civil Disturbance | _____ | _____ |
| Terrorist activity | _____ | _____ |
| Military threat | _____ | _____ |
| Military surge transportation | _____ | _____ |
| Evacuation | _____ | _____ |

E. If yes, are these drills part of a port-wide exercise? _____ _____

Which agency is the initiator?_____

**4. SECURITY PROGRAM** **Y** **N**

A. Does your company/agency have an established security program? _____ _____

B. Does an organizational chart of the security infrastructure exist which lists all security elements within the company/agency and all outside support points of contact (law enforcement, rescue, FBI, Customs, INS etc.)? (Please attach if available.) _____ _____

C. Does the current program address traditional security procedures:

| | | |
|---|---|---|
| Fire | _____ | _____ |
| Theft | _____ | _____ |
| Pilferage | _____ | _____ |
| Sabotage | _____ | _____ |
| Vandalism | _____ | _____ |
| Smuggling | _____ | _____ |
| Cargo tampering | _____ | _____ |
| Civil disturbance | _____ | _____ |

D. Does the current program address extraordinary security measures:

| | | |
|---|---|---|
| Stowaways | _____ | _____ |
| Piracy | _____ | _____ |
| Weather | _____ | _____ |
| Civil Disturbance | _____ | _____ |
| Environmental catastrophe | _____ | _____ |
| Hi-jacking | _____ | _____ |
| Hazardous materials response | _____ | _____ |

E. Does the current program address actual or threatened terrorist activity:

| | | |
|---|---|---|
| Cargo tampering | _____ | _____ |
| Cargo destruction | _____ | _____ |
| Vehicle destruction (hull, truck, train, pipeline) | _____ | _____ |
| Facility destruction | _____ | _____ |
| Threats to personnel in surrounding or transited communities | _____ | _____ |
| Threats to transportation infrastructure (highways, railroads, waterways, pipelines) | _____ | _____ |
| Threats to sensitive environmental areas | _____ | _____ |
| Explosives, nuclear, biological and chemical agent (ENBC) procedures | _____ | _____ |

F. Does the current security program include information security provisions to safeguard electronic business transactions? _____ _____
If yes, by what means?

| | Y | N |
|---|---|---|
| G. Does the current program address/establish physical security standards throughout the shipment, including security during initial and final transfer. | _____ | _____ |
| H. Do these standards apply to facilities owned by other parties (rail cars, containers, barges, tank trucks, etc.) that are used as part of the transportation process? | _____ | _____ |
| I. Do these standards include periodic inspection of all elements (containers, elevators, tanks, rail cars, cranes, yards, etc.) for evidence of tampering, sabotage, theft or attachment of additional items into valid shipments or shipping platforms. | _____ | _____ |
| J. Do the security procedures address threats introduced into the facility by | | |
| Rail assets | _____ | _____ |
| Pipeline | _____ | _____ |
| Ships | _____ | _____ |
| Barges | _____ | _____ |
| Suppliers | _____ | _____ |
| Motor Vehicles | _____ | _____ |
| Labor | _____ | _____ |
| Visitors | _____ | _____ |
| K. Do you conduct security inspections of all elements transiting your facility/system (s)? | _____ | _____ |
| L. Do you rely on the security standards of equipment owners (for leased and third party owned elements transiting the facility/system)? | _____ | _____ |
| M. Do you have copies of the security standards that apply to all transportation elements that transit your system(s) including parent company security policy and practices for third party and leased equipment. | _____ | _____ |
| N. Do these standards address cargo integrity monitoring: | | |
| During transfers? | _____ | _____ |
| During stowage? | _____ | _____ |
| At layovers during transit? | _____ | _____ |
| O. Has your company/facility ever been the subject of a terrorist threat? | _____ | _____ |

## 5. SECURITY HISTORY

A. What is the approximate cost of cargo loss to your company over the last three years (if data is available):

B. Please rank the causes of cargo loss to your company (from 1 - highest, to 8 - lowest):

_____Due to theft
_____Due to pilferage
_____Due to stowaways
_____Due to smuggling
_____Due to civil disturbance
_____Due to threatened terrorist activity
_____Due to actual terrorist activity
_____Due to piracy

C. Given current levels of security, what is your estimate of the threat to cargo, transportation facilities and surrounding civilian communities due to the following:

| | High | Medium | Low |
|---|---|---|---|
| Theft | _____ | _____ | _____ |
| Pilferage | _____ | _____ | _____ |
| Stowaways | _____ | _____ | _____ |
| Smuggling | _____ | _____ | _____ |
| Civil disturbance | _____ | _____ | _____ |
| Terrorist activity | _____ | _____ | _____ |
| Piracy | _____ | _____ | _____ |
| Other (describe)_____ | _____ | _____ | _____ |

D. At what point in the intermodal system is cargo most vulnerable to loss and why?

E. Are certain geographical areas or ports more prone to suffering losses classified in "A" above? If so where?

F. What are the most significant security problems experienced when transporting intermodal cargo? (Please note if your recommendation is specific to either commercial or military cargo.)

G. What recommendations would you make to increase the security intermodal cargo shipments? (Please note if your recommendation is specific to either commercial or military cargo.)

CONFIDENTIALITY: If the data submitted is considered to be trade secret or confidential information, you may affix a "limited rights notice" to your response and the government will thereafter treat the data as "limited rights data", as defined in FAR 52.227-14, in accordance with such notice: *Limited Rights Data - These data are submitted with limited rights in response to the request of the U.S. D.O.T./R.S.P.A/Volpe Center in relation to the Transportation Systems Vulnerability Assessment Project. These data may be reproduced and used by the government or its contractors specifically contracted for this project with the express limitation that they will*

*not, without the express written permission of the Company, be used for purposes of manufacture or disclosed outside the government. This notice shall be marked on any reproduction of this data, in whole or in part.*

**List of entities contacted:**

United States Coast Guard G-OPL
United States Coast Guard G-MOR
Maritime Administration
U.S. Customs Service
Organized Crime Drug Enforcement Task Force
Federal Bureau of Investigation
Drug Enforcement Administration
U.S.Marshalls Service
General Services Administration
International Trade Administration
Department of Transportation
Office of Naval Intelligence
Emory Worldwide
Consolidated Freightways
Old Dominion Freight Lines
Overnight Transportation
Schnieder Transport
Tri - State Motor Transit
Conrail
CSX
Norfolk Southern
Union Pacific
Alaska Cargo Transport
American Presidents Lines
International Shipholding
Crowley American Transport
Crowley Marine Services
Diablo Transportation
Farrell Lines
Lykes Brothers
Maersk Lines
Maritime Overseas
Matson Navigation
Sea Land
Totem Ocean Trailer Express
Alabama State Docks
Port of Anchorage
Port of Beaumont
Canaveral Port Authority
Port of Chicago
Cleveland Cuyahoga County Port Authority
Port of Corpus Christi
International Adjusters Ltd.
ABF Freight Systems
Delaware River Port Authority
Port of Detroit
Port of Duluth
Georgia Ports Authority
Port of Houston
Port of Jacksonville
Port of Long Beach
Port of Los Angeles
Maryland Port Authority
Massachusetts Port Authority
Port of Miami
Port of Milwaukee
Port of New Orleans
Port of New York and New Jersey
North Carolina Ports Authority
Port Arthur
Port of Portland (OR)
Port of San Diego
Port of San Francisco
Port of Seattle
South Carolina Port Authority
Port of Tacoma
Port of Tampa
Port of Toledo
Port of Valdez
Virginia Port Authority
American Maritime Officers Assn.
International Logshoremans Assn.
Int. Ord.of Masters, Mates,Pilots
Association of American Railroads
Transportation Institute
National Cargo Security Council
Air Transport Association
American Petroleum Institute
Amer. Assn.of Importers/Exporters
Container and Intermodal Institute
American Society for Industrial Security
Newport Claims Management
Bi State Harbor Carriers
Council of Logistics Management
American Assn of Port Authorities
Kuhne & Nagle
Cigna
National Industrial Trans.League

# Appendix B: Industry Recommendations for Information System Configuration

## Identification and Authorization

### Unique UserID

Assign each user a unique user identification code (userID) for accountability and audibility.

### Invalid ID/Password

Appear to perform the entire user authentication procedure even if the userID or password entered is invalid. Error feedback shall not indicate which part of the authentication information is incorrect.

### Incorrect Login Attempts

Terminate the login session if the user fails to enter the userID and password correctly:
1. After three (3) login attempts.
2. After failed login attempt, the system shall send an alarm message to the system console and/or to the administrator's terminal, and log this event in the audit trail.

### User Account Data

Maintain, protect, and display status information for all active users and user accounts (enabled and disabled).

### Passwords

Require authentication (i.e., passwords, tokens, biometrics) to login. When passwords are used :

1. Minimum password length: six characters
2. Minimum password complexity: at least one alphabetic and at least one numeric (e.g., 5,7) or special (e.g., #,+) character.
3. Listing of excludable passwords (e.g., common names).
4. Do not indicate to user if she/he has chosen a password already associated with another user
5. Store passwords in a one-way encrypted form.
6. Do not transmit unencrypted passwords over the network
7. Limit access to encrypted passwords, if any, to system administrators
8. Automatically suppress or fully blot out the clear-text representation of the password on the data entry/display device.
9. Prohibit logins without passwords (i.e., null passwords).
10. Permit only authorized administrators to set/reset temporary passwords (which users must change on first login).
11. Require users to change their passwords at least every 180 days (if users are authorized).
12. Require system administrators to change passwords at least every 30 days.

13. Prohibit the reuse of passwords by the same user for at least six months.
14. Provide an automatic capability for ensuring the complexity of user-entered passwords that meets the following:

## System Warnings

### Warning banner

Display, prior to initiating the system login procedure, the warning banner, regarding keystroke monitoring,, unauthorized use, and consequences.

### Concurrent login sessions

Limit the number of times a single user can log into the system from different workstations. The default is a single login session.

### User Access Profile

Grant system entry to a user only if the system administrator has created a user access profile.

### Time Restrictions

Allow or deny system entry based on specified ranges of time:

- Time-of-day
- Day-of-week
- Calendar dates

### Port of Entry

Allow or deny system entry based on means or port of entry:

- Specify the users authorized to access the system via dial-up lines.
- Specify the location (e.g., workstation) from which a user may have access to the system.
- Specify the privileges a user has for ports of entry (e.g., limited to "Read-Only" for dial-in access).
- External networks connect through a controlled point of entry such as a firewall (IP filters, etc.).

### Check for Prior Unauthorized Users

Upon a user's successful entry into the system, the system shall display the following to the user and shall not remove it without user intervention.

- Date and time of the userID's last successful entry into the system;
- Means of access and port of entry of the userID's last successful entry to the system;

- Number of unsuccessful attempts to access the system since the last successful entry by that userID.

### User Inactivity (Timeout)

Terminate an interactive session after an administrator-specified interval of user inactivity. The default shall be fifteen minutes.

### User Access Form

Have each user sign a "User Access Authorization/Revocation" form.

## Access Control

### Authenticated users only

Permit only authenticated user-IDs to have access to the system and its resources.

### Basic Access Control

System administrators shall define and control the access of subjects (e.g., users, groups) to objects (e.g., directories, files, resources) using defined access rights (e.g., read, write, execute).

### Groups

Provide group capabilities to:

- assign access rights to group identities
- associate a user identifier with one or more groups
- display and modify the users in a group

### Access Control List

For each object requiring control, provide an access control list, which specifies the minimum users/groups that need access and their specific access rights (e.g., read write, create, delete).

### Administrators/owners

Restrict the creating/modifying/deleting/revocation of access control privileges by authorized administrators only and owners of specific objects.

### Check Access Rights

Check a userID's access rights to an object, at a minimum, when access to that resource is initiated.

### Security Audit Trail

Create, maintain, and protect a security audit trail of user and administrator actions so that security relevant events can be traced to a specific user for accountability.

### Events Recorded

At a minimum, cause a record to be written to the security audit trail for at least the following events:

- User logins, both successful and failed.
- Attempts to access objects (e.g., resources) or perform functions that are denied by lack of privileges or rights.
- Successful accesses to security-critical objects (e.g., data with high sensitivity).
- Changes to users' security privileges/profiles.
- Changes to the system security configuration.
- Modification of system-supplied software.
- Creation and deletion of objects.

### Event Data

For each recorded event, the audit record shall identify, at a minimum:

- Date and time of the event.
- UserID and associated point of physical access (e.g., node, port, network address, or communication device.
- Type of event.
- Names of resources accessed.
- Success or failure of the event.

### Passwords

Do not record passwords in the security audit trail.

### Alternate Storage Area

Provide for automatic copying of security audit trail files to an alternate storage area after a specified period of time (e.g., so that files are not inadvertently copied over in the event of a full buffer).

### Reports

Generate audit trail reports on a periodic basis or as immediately needed (e.g., when a system alarm detects a security problem).

## Security Management

### Installation

Provide an installation capability for initializing security-related parameters before user attributes are defined.

### Maintenance Mode

Distinguish between normal mode of operation and maintenance mode, and provide a maintenance-mode mechanism for recovery and startup.

### Display/Modify

Provide security controls for displaying and modifying the security policy parameters (e.g., identification, authentication, system entry and access control parameters for the entire system and for individual users.

### Systemwide Set-up

Have a capability to define the identification and authentication parameters on a system-wide basis (e.g., password minimum and maximum lifetime, password length and complexity).

### Restricted Access

Provide restricted access capabilities for displaying, modifying, or deleting user account information.

### User Attributes

Provide a means to uniquely identify: (1) security attributes for a user, and (2) all the users associated with an attribute and (3) definition and maintenance of groups.

### Define/Maintain Security Controls

Be capable of defining and maintaining the security controls for subjects (e.g., users, groups) and objects (e.g., directories, files, resources) using defined access rights (e.g., read, write, execute).

### Maintenance

Provide security controls for routine control and maintenance of system resources: enabling and disabling of peripheral devices, mounting of removable storage media, backing-up and recovering user objects; maintaining the system hardware and software elements (e.g., on site testing); and starting/shutting down the system.

## Other Protected Features

### Trusted Path

Generate a trusted communication path between itself and the user for initial identification and authentication. Communications via this path shall be initiated exclusively by a user.

### Logical System Protection

Operating system isolation/protection from external interference and tampering (e.g., by reading or modification of its code).

### System Self-Checking

Features to validate correct operation of hardware/firmware, including: power-on tests, load tests, and operator-controlled test.

### System Initialization and Recovery

Ensure security features are fully restored

### Unix and Solaris Technical

*a.* Have all non-required services been removed from internet daemon, *inetd.conf.*
b. File Transfer Services: Has *.netrc* been banned from clients' home directory.
**c.** Has *root* been placed in */etc/ftpusers* or */usr/etc/ftpusers* to prevent *root* from logging in using FTP.
**d.** Has *sendmail* been removed.
**e.** Has *.telnetrc* been banned from clients' home directory.
**f.** Has *rhosts* been disabled.
**g.** Has *rlogind* been disabled.
**h.** Has *rshd* or *remshd* been disabled.
**i.** Has *fingered* been disabled.
j. Have all security patches been installed.

# Appendix C: Industry Recommendations for Security Audit

1. **SECURITY**
   A. Supplier confirms that employees of Supplier performing work at Buyer's facilities have no record of criminal convictions involving drugs, assaultive or combative behavior or theft within the last five years. Supplier understands that such employees may be subject to criminal history investigations by Buyer at Buyer's expense and will be denied access to Buyer's facilities if any such criminal convictions are discovered.
   B. Within fifteen (15) days after executing of this Agreement, Supplier shall furnish Buyer with its plan to provide an atmosphere of restricted accessibility for Buyer freight while in Supplier's control. Furthermore, where restricted accessibility may be precluded bylaw, Supplier agrees to implement Buyer's Minimum Security Guidelines. Supplier shall follow generally accepted industry standards to do so. Supplier agrees to ensure a level of security acceptable to Buyer at all times.
   C. Buyer must be notified immediately of any Supplier inspections.
   D. If exception is taken or signs of tampering spotted in any portion of a shipment, Supplier will immediately notify Buyer and will proceed according to the instructions provided by Buyer personnel. If material is to continue transit, reasonable efforts must be made to preserve evidence of tampering, i.e., photographs.
   E. Supplier and its agents' facilities shall be secure from unauthorized entry. Buyer may, at its option, periodically audit Supplier's facilities and may require Supplier to jointly audit any agents' facilities.
   F. Supplier agrees to confirmed comply with requirements and responsibilities as defined in Addendum "D", Freight Contractors Minimum Security Guidelines.

**ADDENDUM**

# FREIGHT CONTRACTORS INDUSTRY RECOMMENDED MINIMUM SECURITY GUIDELINES

## 1. GENERAL

A. The Supplier shall produce to Buyer's local Distribution Contracts and Security Manager, written security procedures and evidence of implementation based on Buyer's security guidelines, within one month after commencement of the contract or freight agreement.

B. The Supplier agrees to assign a senior security representative to monitor, standardize and implement its security procedures throughout all servicing and transit locations

C. The Supplier shall ensure that all employees and sub-contractors who have access to Buyer product are positively vetted before employment commences. Evidence of vetting procedures to be produced at Buyer's request. Compliance with this section will be governed by existing local laws and regulations.

## 2. HANDLING GUIDELINES

A. The Supplier is required to provide a secure storage area for Buyer product. The secure area will be designed to deter and prevent unauthorized access. Entry to the secure area is to be limited to personnel directly involved in shipping and receiving of Buyer's product. For the purpose of this action, examples of security storage may include sealed or locked containers, locked cages, locked hard-wall areas, and cargo stored in racks at a sufficient height to prevent access by unauthorized persons. Any loose cargo stored over six hours must be stored in a locked cage or locked hard-wall area.

B. Loading of Buyer product shipments must be done in the presence of the authorized driver; no pre-loading of product shipments on vehicles for later collection is permitted.

C. The Supplier is prohibited from opening Buyer freight unless directed by Customs officials or Buyer. Any freight showing evidence of being opened or tampered with must be reported to Buyer immediately and a written report is to be produced within twenty-four (24) hours following the discovery. The Supplier must implement procedures for communicating freight discrepancies and damaged cartons to Buyer.

## 3. SUPPLIER'S PREMISES SECURITY

A. The Supplier will provide and maintain, at all times, adequate security systems to allow continuous security monitoring and protection of Buyer's freight against fire and intrusion. This will include a building fire detection system, an intruder detection system, and a closed circuit television system with a video recording capability. Any exceptions to this requirement must be approved by Buyer.

B. The Supplier will ensure that all vehicle and pedestrian access to its premises is controlled to prevent unauthorized casual and intentional intrusion. Details of measures shall be included in Supplier's security procedures.

4. **VEHICLE SECURITY**
   A. All trailers used for transporting product shall be quipped with solid sides and locking cargo doors. Any exception to this requires prior written agreement by Buyer. Any such waivers granted by Buyer shall be on an individual shipment basis and will not cover multiple shipments of Buyer's product.
   B. Where applicable, the driver of the delivery vehicle shall not deviate from the assigned delivery routes nor make unscheduled stops.
   C. Buyer reserves the right to require, at any time, that the Supplier's vehicle tractor units and trailers be fitted with a mutually agreed vehicle location system and that arrangements be made to supply Buyer with copies of alarm exception reports.
   D. All Supplier's vehicles used for carrying Buyer product shall be equipped with a suitable communication system that will allow the vehicle driver to request assistance in the event of an emergency.

5. **AUDITS**
   A. Excepting routine business meetings with Buyer, Supplier will meet with Buyer Security or its appointed representatives at least one per year or at Buyer's request.
   B. Buyer reserves the right to audit any of Supplier's premises and/or servicing and transit locations and will report audit results and proposed corrections within fifteen days of completed audit. Copies of audit procedures shall be included in Supplier's security procedures.

6. **CARRIER'S USE OF SUB-CONTRACTORS**
   If the agreement of the parties fails to address Supplier's use of sub-contracts for performance of any of its freight forwarding responsibilities under this base contract, then Supplier must seek and receive Buyer's written consent before use of such sub-contractor.

7. **GENERAL SECURITY RESPONSIBILITIES**
   A. Supplier corporate security representative will complete loss/theft investigations and report to Buyer in writing within 24 hours of any such incident.
   B. Supplier will perform twice a year self audit of facilities in cities as well as hub locations through which Buyer's freight is moved and report results to Buyer in writing according to Buyer's security checklist.
   C. Supplier will establish security Standard Operating Procedures for Buyer's shipments by March 1, 1994 and update it twice per year. Supplier will provide a copy of its security Standard Operating Procedures to Buyer immediately after promulgation and after each update. Supplier will perform additional updates as needed.
   D. Buyer Corporate Security to have open access to Supplier facility audits and loss/theft investigations. Also, Buyer's Corporate Security shall, as necessary, participate with Supplier security on security investigations and resolutions of issues involving loss/theft investigations.
   E. As needed, Supplier to provide Buyer a full report on all losses and thefts at specific facilities for indicated period of time (6, 12, and 24months...etc.). Supplier's report will list losses for both Buyer and non-Buyer freight.

F. Supplier will comply with Buyer's Freight Carrier Contractors Minimum Security Guidelines. A blanket exception will be allowed on item 4.C (vehicle locator system) provided Supplier's vehicles are equipped with two way radio (minimum requirement) equipment. Any other exceptions to Buyer's Security guidelines will be considered by Buyer on a location by location basis. Buyer reserves authority to accept or refuse exception requests.

G. Quarterly Security Reviews shall be conducted at each servicing location. Results are to be reported at quarterly meetings and any irregularities and corrective action plans explained.

H. Supplier's Corporate Security Official will meet with Buyer's Security semi-annually or as required. A security report will be submitted as required, with copies provided to Buyer's Security and to Buyer's Corporate Logistics.

I. Airport audits will be performed by Supplier on a regular basis as per local Buyer requirements. Local Supplier Security Officials and local Buyer Security Officials will meet on a regular basis as per local security requirements.

**ANY AMENDMENTS OR WAIVERS TO THESE GUIDELINES MUST BE APPROVED BY CORPORATE SECURITY AND CORPORATE LOGISTICS**

## Ownership

The high value product/inventory program clearly defines the primary responsibility for the security and control of high value product/inventory. The responsibilities of logistics/security and site management include:

(1) Logistics to own the security audits of warehouses which they manage.
(2) Logistics will also own the security audits of freight lanes managed by Buyer as defined in Exhibit One in the appendix of this policy
(3) Corporate Security resources to provide training and timeline for training.
(4) Ownership for standardization for security processes and material
(5) Buy off of document to be used for security audit guidelines

Areas where Logistics cannot own:

(1) Material warehouses as defined in Exhibit Two
(2) Inbound materials not routed on freight suppliers

# FREIGHT CARRIER CONTRACTORS
# INDUSTRY RECOMMENDED
# MINIMUM SECURITY GUIDELINES OVERVIEW

## 1.0 OVERVIEW

1.1 Security is establishing a program to insure the safe transportation of products ("Program") throughout the world. This Program sets procedures and controls on the way HVP products are packed, collected, transported and delivered. One example of protecting products shipped to customers from being stolen is through the use of different freight carriers.

1.2 The Program establishes the responsibilities of each of the departments charged with Shipping, Security, Risk Management, selecting Freight Suppliers and selecting independent Security Consultants.

1.3 To encourage Freight Suppliers to comply with and actively participate in the implementation of the Program..

1.4 To educate Security of the volumes, routes, distribution centers and modes of transportation used in the distribution and transportation of HVP products. Security will ensure that these conform with the minimum Freight Security Guidelines ("FSG" ) established by the Program.

1.5 Logistics to actively monitor and enforce the Program by audits, spot checks and when losses occur, investigations.

## 2.0 SCOPE

This Program applies to:

2.1 All facilities throughout the world having distribution or shipping/delivery responsibilities.

2.2 All freight suppliers and couriers.

2.3 All freight shipped by company or shipped on behalf of its customers.

## 3.0 RESPONSIBILITIES

3.1 **International Security Management and Corporate Security are responsible for**:
Implementation of existing procedures.
Reviewing and updating procedures.
Providing support to the Distribution/Shipping and logistics departments
Investigations
Audits of contracted security or consultants, where applicable

3.2 **Site Distribution Department and Corporate Logistics are responsible for**:
Implementation or procedures
Self audit
Security for forwarding
Routing information
Shipment volumes and values
Providing Risk Management with claims information
Providing Site and Corporate Security with discrepant freight reports
Conducting scheduled audits-yearly unless a theft occurs, of which then scheduled audits will be done quarterly

3.3 **Corporate Security is responsible for**:
The implementation of the Freight Security Program
Informing Distribution/Logistics departments of concerns or situations that may adversely affect operations
Conducting scheduled annual audits
Providing consulting support to international and domestic Security Management, Distribution departments and Logistics.

3.4 **Suppliers are responsible for**:
Complying with the requirements of the FSG
The safe and secure movement of product to final destination.
Compliance by subcontractors with the FSG
Quarterly audits at freight terminal facilities they use when shipping products for Buyer.

# FREIGHT CARRIERS MINIMUM INDUSTRY RECOMMENDED SECURITY GUIDELINES

## 1.0 SCOPE

The Freight Security Guideline program has been established to insure the safe transportation of products throughout the world. The successful implementation of the Freight Security Guideline program is dependent upon freight suppliers and company working in partnership. Primary responsibility for safe and secure transportation of products lies with the freight supplier or their subsidiaries, subcontractors, and with the Logistics organization. The freight suppliers minimum security guidelines will be incorporated into any contract between the supplier and Buyer and into the suppliers own security program.

The requirements of this guideline shall apply to all geographical areas. In geographical areas where English is not the first language, this document will be translated into the language of that country. It is incumbent upon the supplier to insure that every employee has been trained or familiarized with these guidelines.

## 2.0 GENERAL

Within thirty days of acceptance of the contract, the supplier shall submit, to the regional representative of Logistics organization, Security Management, a copy of the suppliers own security procedures. Security procedures must comply with FSG requirements and will not be in conflict with those requirements. In cases where the suppliers security procedures do not meet minimum FSG requirements, any of the following actions may be taken:

a. The supplier shall present a written action plan, outlining corrective actions and implementation dates.

b. Logistics may issue a written waiver specifying requirements of the FSG which are not applicable. However, the supplier is required to meet all portions of the FSG which have not been waived.

c. In extreme cases, the supplier may be placed on a formal Corrective Action Plan as described in the contract between company and the supplier.

Company shall have the right, prior to or after entering into a contractual agreement with the supplier, to conduct a risk assessments on a regularly scheduled basis and as determined by company of the suppliers transit, storage or handling locations, vehicles and processes or procedures.

## 3.0 PROCEDURE

### 3.1 SECURITY REPRESENTATIVE:

The supplier will designate a representative to liaison with company representatives, including Logistics, Site Traffic, Corporate and Site Security. It is the designated security representatives responsibility to insure that FSG requirements are incorporated into the suppliers own security program. The security representative will monitor the effectiveness of the program by conducting self audits and risk assessments.

### 3.2 CONDUCTING EMPLOYEE BACKGROUND CHECKS (VETTING):

A background check includes a review of the employee/applicants prior employment and driving and criminal history for a period of five years. The supplier shall perform a drug test and background check on any employees or contractors handling, storing, or transporting buyer product unless specifically prohibited by local law. The background investigation process will be incorporated into the suppliers FSG and applies to all present or prospective employees. The supplier shall provide evidence of such background checks to company representative upon request.

Compliance with this requirement shall be governed by local laws and no action to comply is to be in conflict with those laws or regulations.

3.3 SUPPLIERS, SUBSIDIARIES AND CONTRACTORS PREMISES:

The supplier, their subsidiaries, or contractors shall provide and maintain adequate security measures at any facility that handles or stores company products or materials. Adequate security measures include, as minimum the following:

a. Intruder detection system.
b. Closed circuit television(CCTV), recording and monitoring system. The CCTV systems need to be operable, in good working condition, with all parts intact.
c. Fire detection/suppression system.
d. Controlled access to vehicles and pedestrians.
e. Secure storage location(s) for HVP product delayed in transit for a period longer than six hours. (see section 3.4 for details of this requirement)
f. Secure environment (a-e above), within which vehicle loading or unloading is carried out.

The supplier is required to notify Logistics and Corporate Security of any changes to the suppliers facility, physical location, or security system that will significantly affect the overall security program.

3.4 STORAGE OF FREIGHT AT THE SUPPLIERS FACILITY:

The supplier shall insure that all freight that will be in the suppliers facility for more than six hours will be placed in a secure storage area. This area will be sufficient to deter and prevent unauthorized access. The entry procedure must include a method to establish the identity of persons (names and addresses) who have entered the secure area. Examples of such controls include key logs and card reader access list. Under some circumstances, product stored in racks at sufficient height to prevent access may meet the provisions of this requirement. However, the decision to approve the method lies solely with company.

3.5 SCHEDULED ROUTES, LOADING, TRAINING AND PRE-ALERTS:

3.5.1 The supplier shall use routes and schedules (published and well traveled) which maximize overall freight security. Suppliers will not permit any deviation except to exceptional circumstances, i.e. floods and road or traffic conditions that create excessively long delays, mandatory detours, or other causes that are justifiable. Unscheduled stops are not permitted.

3.5.2 Supplier shall implement a system to insure that the driver is present when product is loaded. Loading of vehicles in advance of immediate departure is prohibited at supplier's docks. Pre loading at an Buyer site where storage is a problem can be done if approved by Security and Logistics.

3.5.3 Drivers shall be trained to respond to threatening situations. This includes robbery, theft or hijacking. Training must emphasize that the safety and survival of the driver or others is of the highest priority.

Suppliers shall provide to company a proof of such training undergone by drivers during the audit

3.5.4 Suppler will incorporate a pre-alert system under circumstances of unusually high value cargo or expedited deliveries ("hot" shipments).

a. Where high value unit (hvu) cargo is regularly carried, the vehicle or trailer unit shall be equipped with a tracking system which will enable the supplier to monitor its movement throughout the journey (Global Positioning Satellite or other)

b. Additionally, any consignment or single vehicle load which has HVP product with value in excess of US $10,000,000 will be provided with an escort vehicle for the duration of the journey. In areas where allowed by law, the escort will be armed with protective weapons.

3.6 HIGH VALUE LOADS - US $XXX OR MORE:

When transporting loads with a value of $XX or more, the supplier will conform with company's procedures for HVU security. Additionally, procedures will include, where relevant and feasible:

3.6.1 Provision of escort vehicle(s), equipped with adequate means of communication

3.6.2 Two drivers per vehicle, to permit non stop, long distance journeys if required.

3.6.3 Double manned vehicles to be equipped with two tachographs, as per legal requirements.

3.6.4 Vehicle tracking system.

3.6.5 Management by vendor throughout the collection/transit/delivery period.

3.6.6 Movement progress reports to Security/Logistics.

3.6.7 Control of all vehicle communications.

3.6.8 A written contingency plan covering, hijack, attempted robbery, breakdown etc.

3.6.9 Full written details of proposals to be submitted to Logistics and Security, prior to carrying out any improvements.

3.7 RISK ASSESSMENTS AND AUDITS:

Acceptance of a contract between company and the supplier is implicit of company's right to conduct risk assessment or audits at the suppliers facility, subcontractors facility or transport vehicles used to carry HVP product or material. Logistics shall inform the supplier or assessment/audit results with twenty working days from completion of audit report. Due dates for completion of corrective actions shall be negotiated between Logistics and the supplier. However, corrective actions cannot exceed sixty days.

3.8 REPORTS OF THEFT, LOST OR DAMAGED PRODUCT OR INVENTORY:

The supplier shall actively cooperate with law enforcement authorities, Logistics, and Security representatives or their appointed agents in conduct of an investigation of product or material that is lost, stolen or pilfered, damaged or tampered with while in the possession of the supplier. Logistics and/or Security will contact law enforcement authorities immediately upon notification of an investigation.

A reported procedure shall be included in the suppliers own freight security guideline. The required time for reporting incidents involving company product or material to the local representative is within twenty-four (24) hours of discovery. The supplier will provide frequent updated information to Logistics and Security concerning the status of any investigation.

SUPPLIER FREIGHT SECURITY RISK ASSESSMENT

SUPPLIER NAME_____
REPRESENTATIVE_____

SUPPLIERS LOCATION_____AUDIT
DATE_____

| FSG NO. | STATUS (Satisfactory or Improvement Required) | ACTION ** |
|---|---|---|
| | | |
| 1.0 SCOPE (FSG/in suppliers program) | | |
| | | |
| 2.0 GENERAL | | |
| a. Written security procedures? | | |
| b. Written corrective action plan? | | |
| c. Waivers required? | | |
| d. CAP required? | | |
| | | |
| 3.0 PROCEDURE | | |
| 3.1 Security liaison appointed? | | |
| 3.2 Employee background checks | | |
| 3.3 Minimum security measures | | |
| 1. Intruder detection system? | | |
| 2. CCTV and recorder? | | |
| 3. Fire detection system? | | |
| 4. Controlled access? | | |
| 3.4 Storage of freight | | |
| 1. Secure storage area? | | |
| 2. Key control/log? | | |
| 3. High bay racking? | | |

| |
|---|
| 3.5 Vehicles |
| 1. Alarm/immobilize? |
| 2. Communication system? |
| 3. Solid side/roof? |
| 4. Lockable doors? |
| 5. Security seals (numbered)? |
| 6. Scheduled (firm) routes? |
| 7. Driver/employee training? |
| 8. Preloading prohibited? |
| 9. Prealert for high value cargo? |
| 10. FSG language translation? |
| |
| 3.6 Audits |
| 1. Quarterly self-audits? |
| |
| 3.7 Losses & Damage |
| 1. Documented procedure? |
| |

| LIST OF ACTION ITEMS | | | |
|---|---|---|---|
| FSG NO. | ITEM | REQUIRED ACTION | OWNER/DUE DATE |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## SECURITY AUDITS
## RATING SUMMARY

**Audit rating score criteria:**

**A security "Preventive Measure" is defined as a specific prevention/protection strategy, device, or physical element. These Preventive Measures are detailed in each "Area of Concern" section of the security audit format.**

**The presence or utilization of a listed security Preventive Measure should be evaluated using a sliding scale, rating the presence and integrity of the Preventive Measure in regard to the audit being performed. In determining a rating score of a security Preventive Measure, the following descriptions of the necessary elements/performance levels should be used:**

| POINT VALUE | DESCRIPTION OF ASSESSMENT CRITERIA |
|---|---|
| 0 | Preventive Measure not present or utilized--no plans to adopt or implement |
| 1 | Preventive Measure infrequently and irregularly present or utilized, or in poor operating condition--no plans for enhancement or improvement |
| 2 | Preventive Measure present or utilized on occasional/irregular basis, or in questionable/inconsistent working order |
| 3 | Preventive Measure generally present or utilized, with occasional gaps/lapses in performance evident--plan in progress to improve, and routine self-audit of performance |
| 4 | Preventive Measure present or utilized, with strong and consistent integrity in use/efficiency--performance is routinely self-audited |
| 5 | Preventive Measure exceeds requirements, is firmly in place and adopted as standard business practice; regularly self-audited for performance with focus on continuous improvement |

AUDITORS: Date of Audit:

LOCATION AUDITED: ***CONFIDENTIAL INFORMATION***

| AREA OF CONCERN | PREVENTIVE MEASURES | RATING OF IMPORTANCE (1-5) | X if not scored | AUDIT SCORE (1-5) | ADJUSTED SCORE (Importance x audit score) | COMMENTS |
|---|---|---|---|---|---|---|
| **Perimeter Security** | 1. Enclosed pad area (fence 8' height minimum) | 4 | | | 0 | |
| | 2. Intrusion and panic alarms monitored 24X7 | 5 | | | 0 | |
| | 3. CCTV coverage of critical access points | 5 | | | 0 | |
| | 4. All exterior openings > 96 square inches secured with alarm or barrier | 5 | | | 0 | |
| | 5. Gate control (tire spikes, barrier poles, remote closure, etc.) | 2 | | | 0 | |
| | 6. Exterior lighting | 3 | | | 0 | |
| | 7. Steel post crash barricades installed at windows | 1 | | | 0 | |
| | 8. Ground level windows secure (steel mesh/bars, alarm) | 2 | | | 0 | |
| | 9. Street access clearly marked with address information | 1 | | | 0 | |

Total: 0 140 possible

| AREA OF CONCERN | PREVENTIVE MEASURES | RATING OF IMPORTANCE (1-5) | X if not scored | AUDIT SCORE (1-5) | ADJUSTED SCORE (Importance x audit score) | COMMENTS |
|---|---|---|---|---|---|---|
| **Access Control/ Office Areas** | 1. Main office entrance security (guards/receptionist, access controls, panic alarm, etc.) | 5 | | | 0 | |
| | 2. Visitor sign-in/badging | 4 | | | 0 | |
| | 3. Off hours office access control | 5 | | | 0 | |
| | 4. Terminated employee access removal procedures | 5 | | | 0 | |
| | 5. Building alarm access restricted (code #'s, key personnel | 5 | | | 0 | |
| | 6. Limited access to dock areas | 5 | | | 0 | |
| | 7. Visitor escort policy | 3 | | | 0 | |
| | 8. Facility entry/exit inspection policy | 2 | | | 0 | |
| | 9. Employee picture badge | 2 | | | 0 | |

Total: 0 180 possible

| AREA OF CONCERN | PREVENTIVE MEASURES | RATING OF IMPORTANCE (1-5) | X if not scored | AUDIT SCORE (1-5) | ADJUSTED SCORE (Importance x audit score) | COMMENTS |
|---|---|---|---|---|---|---|
| **Facility: Dock / Warehouse** | 1. Incoming traffic screened for identity, authorization | 5 | | | 0 | |
| | 2. All doors kept closed and secured when not in use | 5 | | | 0 | |
| | 3. Drivers/unauthorized personnel restricted to loading dock/manifest area | 5 | | | 0 | |
| | 4. HVP secured in locked hardwall or cage area CCTV coverage Limited and recorded access (log/list) | 5 | | | 0 | |
| | 5. No pre-loading of trailers. | 3 | | | 0 | |
| | 6. No employee parking in controlled area. | 3 | | | 0 | |
| | 7. Outgoing Trash inspection | 3 | | | 0 | |
| | 8.CCTV recording equipment maintained in secured location, tape rotation ≥ 30 days | 5 | | | 0 | |

Total: 0 170 possible

| AREA OF CONCERN | PREVENTIVE MEASURES | RATING OF IMPORTANCE (1-5) | X if not scored | AUDIT SCORE (1-5) | ADJUSTED SCORE (Importance x audit score) | COMMENTS |
|---|---|---|---|---|---|---|
| **Security Operations** | 1. Security liaison appointed, informed and fully engaged in security management. | 5 | | | 0 | |
| | 2. Security policies/procedures documented, all employees familiarized. | 5 | | | 0 | |
| | 3. Incident (loss, damage,etc.) reporting system timely and effective | 5 | | | 0 | |
| | 4. Self-audit process | 4 | | | 0 | |
| | 5. Sub-contractor audits | 5 | | | | |
| | 6. Indicators (loss,incidents,problem areas, etc.) identified, tracked, recorded. | 4 | | | 0 | |

Total: 0 140 possible

| AREA OF CONCERN | PREVENTIVE MEASURES | RATING OF IMPORTANCE (1-5) | X if not scored | AUDIT SCORE (1-5) | ADJUSTED SCORE (Importance x audit score) | COMMENTS |
|---|---|---|---|---|---|---|
| **Employees** | 1. Employee background check in place | 5 | | | 0 | |
| | 2. Employees provided robbery response training | 5 | | | 0 | |
| | 3. Drivers provided robbery and hijacking response training | 5 | | | 0 | |
| | 4. Panic alarms tested and training provided | 2 | | | 0 | |

| | | | |
|---|---|---|---|
| Total: | 0 | 85 | possible |
| **Grand Total:** | **0.00** | **990** | **possible** |
| | **or** | **0.00%** | |
| | | **Not Acceptable** | |

| AREA OF CONCERN | PREVENTIVE MEASURES | RATING OF IMPORTANCE (1-5) | X if not scored | AUDIT SCORE (1-5) | ADJUSTED SCORE (importance x audit score) | COMMENTS |
|---|---|---|---|---|---|---|
| **Freight In Transit** | 1. Pre-alerts for HVP | 5 | | | 0 | |
| | 2. 24 hour notification of lost/missing freight | 5 | | | 0 | |
| | 3. Hard-sided cargo containers | 5 | | | 0 | |
| | 4. Cargo container area secured | 4 | | | 0 | |
| | 5. Integrity verification/ reconciliation (weight, piece count) at each transit point | 5 | | | 0 | |
| | 6. No staging of HVP @ airport w/o protective measures (secured cage,CCTV,guards ) | 5 | | | 0 | |
| | 7. Vehicle movement tracked/traceable (GPS, mobile radio, phone) | 3 | | | 0 | |
| | 8. Vehicle immobilization devices in place | 3 | | | 0 | |

Total: 0 175 possible

| AREA OF CONCERN | PREVENTIVE MEASURES | RATING OF IMPORTANCE (1-5) | X if not scored | AUDIT SCORE (1-5) | ADJUSTED SCORE (importance x audit score) | COMMENTS |
|---|---|---|---|---|---|---|
| **Information Systems** | 1. General access to information of contents/routes/storage of HVP controlled and recorded. | 5 | | | 0 | |
| | 2. Password protection in place, routine expiration and mandatory update. | 5 | | | 0 | |
| | 3. Exception reports-errors, missing documents,inventory, damage, etc.-process of preparation, dissemination, and resolution | 5 | | | 0 | |
| | 4. Access to sensitive transactions (shipment contents, value, etc.) Limited to authorized personnel - monitored and recorded. | 5 | | | 0 | |

Total: 0 100 possible

# Appendix D: Defining Terms

To clarify the terms used in this report, this section provides definitions and descriptions to support improved understanding of findings and recommendations.

As used in this report, the *transportation infrastructure assurance concept* is applied to cargo terminals exclusively. To avoid the confusion that occasionally hinders dialogue between multiple modes, the following definition of cargo terminal was used to guide all project activities:

> "An assigned area in which cargo (containerized or non-containerized) is prepared for loading into a vessel, train, truck, or airplane or is stacked immediately after discharge from the vessel, train, truck, or airplane; any area assigned for loading/unloading, temporary storage of vehicles, or the interchange of cargo during transit."

There are hundreds of cargo terminals throughout the United States. Regardless of variations in location, design, and operation, all cargo terminals perform similar functions: cargo transfer operations, cargo staging, modal staging (trailers/tractors/cars/trains), gate operations, storage, and security.

In the United States, cargo transportation is often characterized as a hub and spoke system with cargo terminals providing the vital hubs that concentrate loads for long haul, transfer bulk or break-bulk goods from ship to other modes, or prepare received shipments for local delivery. There are several types of terminals that support cargo operations:

- Ocean Port Container Terminals (the majority of cargo container traffic moves through the top ten U.S. container ports and the approximately 45 terminals operated by these ports)
- Ocean Port Breakbulk Terminals (these terminals support the cargo movement of equipment, machinery, automobiles, military goods)
- Ocean Port Bulk Terminals (these terminals support the movement of dry and liquid commodities)
- Rail-Truck Terminals (these terminals manage container-on-flatcar [COFC] and trailer-on-flatcar [TOFC] transfers)
- Barge Terminals (these terminals manage cargo transfer of bulk goods on inland waterways)

Within cargo terminals, transfer facilities manage the actual movement of cargo from one mode of transportation to another. In the case of container cargo, standardized containers expedite this process, with quick, simple adjustments to release them from one mode and connect them

directly to another (either a rail flatbed, truck chassis, ship, barge, etc.). Requirements for drayage and storage can be minimized by precision delivery scheduling (assuring that the next mode is in place to receive the cargo of the previous one). Roll on - Roll off cargo is simply driven from one mode to the next. Bulk cargoes (liquid or solid) generally are transferred from an intermediate facility such as a tank farm, silo, or storage yard or from a vessel. Break bulk cargo is the most labor intensive and requires removal from one mode, usually by crane or lift, drayage to staging for the next mode (or intermediate storage), and final handling to load the cargo to the next transportation mode.

Definitions for other terms used in industry and government within the transportation and law enforcement areas include the following:

**ACCOUNT PARTY**: The party instructing the bank to open a letter of credit on whose behalf the bank agrees to make payment. In most cases, the account party is an importer or buyer, but may also be a construction contractor or a supplier bidding on a contract.

**AD VALOREM**: "According to the value" Used for customs duties that are fixed as a percentage value.

**ADVISED CREDIT**: A letter of credit that has been advised by another bank without engagement on the part of that bank. An advising bank has the obligation to take reasonable care to check the apparent authenticity of the credit, which it advises.

**ADVISING BANK**: A bank, operating in the exporter's country, that handles letters of credit for a foreign bank by notifying the export firm that the credit has been opened in its favor. The advising bank fully informs the exporter of conditions of the letter of credit without necessarily bearing responsibility for payment.

**ADVISORY CAPACITY**: A term indicating that a shipper's agent or representative is not empowered to make definitive decisions or adjustments without prior approvals of the group or individual represented.

**AGENCIES:** The right given by an individual, body, or firm to another person or company to act on its behalf. An agency may be classified as:

- A specific or special agency where duties are restricted to a specified transaction:
- A general agency where actions are undertaken on behalf of principals, with an amount of responsibility;
- A universal agency which involves full power of attorney provided all actions are within the law. Agency appointments are normally given for a stated period of time or indefinitely by means of a written contract or letter of intent. There is wide scope for the activity of an agency, such as representing

the ship owner, contracting agreements for repairs and dry-docking, acting in the absence of the owners, or importing materials.

**AGENT:** A person or company acting as an AGENCY, authorized to act on behalf of its principal. The agent is very important in that he will be the owner's representative who has to act promptly and effectively to deal with problems. The agent is duty bound to follow the owner's instructions and may indicate on whose authority he is acting. There are many levels of representation characterized as agent, including managing agent or MANAGING OWNER, which may actually be the owner of the ship. Typically the agent handles all formalities for a ship's entry into port, during customs clearance, and up to time of sailing. The agent arranges with the authorities for the allocation of berthing space, advises cargo owners of the availability of the ship or cargo (depending on whether the cargo is for export or import), organizes loading and unloading, and provides for provisioning through a ship CHANDLER.

**AIR WAYBILL**: A document issued by an air carrier or fright forwarder that gives evidence of the shipment and/or delivery of goods for shipment by air. It is non-negotiable and is generally consigned to the buyer, the buyer's agent, or to the seller's local agent.

**ARREST:** An official order enforced as a matter of law against a ship for actions against the laws of the government ordering the arrest, or as a means of enforcing a maritime LIEN.

**AUTHORITY TO PAY**: (Often mistaken for letter of credit) An authority to pay is an advise stemming from a buyer, addressed through the buyer's bank to the seller, by way of the correspondent bank to pay the seller's drafts for a stipulated amount. The Authority to Pay may be canceled or modified before the drafts are presented. Once the drafts drawn on the correspondent bank are paid by it, the seller is no longer liable as drawer. Usually not offered by U.S. Banks.

**AUTHORITY TO PURCHASE**: This document, while similar to the Authority to Pay, differs in that under an Authority to Purchase the drafts are drawn directly on the buyer. They are purchased by the correspondent bank with or without recourse against the drawer. Usually not confirmed by the US bank. Authority to purchase is used primarily in the Far East.

**AWAITING ORDERS:** A ship is awaiting orders when it has not been instructed where it is to discharge its cargo, or when its next employment is undetermined. A ship legitimately DECLARING that it is awaiting orders may be underway (but usually near a discharge port), at anchor in a holding area, or adrift on the high seas outside normal shipping lanes.

**BACK-HAUL:** The return movement of a vehicle from original its destination to original origin.

**BACK-TO-BANK LETTERS OF CREDIT**: A letter of credit supported by ("backed by") a separate letter of credit having nearly identical documentary requirements, but with four features normally differing:
1.Name of the beneficiary
2.Acccount Party
3.Amount
4.Shipping Date

**BALLAST, IN-BALLAST:** A ship is in ballast when it is empty of cargo, but has an amount of (usually) sea water in ballast tanks. This serves to keep the propeller and rudder effectively submerged, and to keep the bows in the water to improve handling and prevent slamming. A ship in ballast may or may not be evenly TRIMMED fore and aft, but will never normally be ballasted so deeply as to approximate the loaded condition; LOAD LINE at or near the water line, A merchant ship on a long voyage will not normally ballast down to replace fuel consumed. Tankers and bulk carriers will normally sail either in an obviously light (ballasted) condition or down to the load line. However, chemical tankers and those carrying refined products will often sail partially loaded. Tankers out of Red Sea ports may sail less than full in order to meet draft.

**BANK DRAFT**: A check drawn by a bank on another bank. This is customarily used when it is necessary for the customer to provide funds which are payable at a bank in some distant location.

**BANKER'S ACCEPTANCE:** A form of credit created when a bank acknowledges in writing on a time draft its obligation to pay face amount to the holder at specific time in the future.

**BANKER'S BILL**: A bill of exchange drawn by an exporter on the importer's bank.

**BAREBOAT CHARTER:** Also known as demise charter. A charter for a long period, where the charterer assumes responsibility for the normal functions of a ship owner; i. e. manning and appointment of officers, payment of running expenses, dry docking, painting, and repair. In some cases, the registry and name of the ship will also be changed. In a bareboat charter, the powers of ownership have been assumed by the charterer, regardless of the registered or beneficial owner of record. In many instances the bareboat charterer becomes the outright owner at the end of the charter period. In others, the owner of the ship through a foreign "paper" company will bareboat charter the ship back to himself, gaining the benefits of control over a ship without having to comply with his own national rules regarding manning and operations. This form of bareboat charter is most common with German owners using Cypriot or Filipino front companies.

**BENEFICIARY**: The party who receives payment upon the conditions stipulated in a letter of credit. This party is usually a seller or an exporter. The person in whose favor a letter of credit is issued or a draft is drawn.

**BILL OF LADING:** The title document issued by a carrier (railroad, steamship, or other common carrier) which serves as a receipt for the goods and is a contract to deliver the goods to a designated person or to his or her order. The bill of lading describes the conditions under which the goods are accepted by the carrier and details the nature and quantity of the goods, name of vessel (if shipped by sea), identifying marks and numbers, designation, etc. The person sending the goods is the shipper or consignor, the company or agent transporting the goods is the carrier, and the person to whom the goods are designated is the consignee. Bill of lading maybe negotiable or non-negotiable.

**BLOCKED ACCOUNTS**: Deposits maintained in a country that does not allow conversion into another currency or removal of the deposits from the country.

**BONDED WAREHOUSES**: A warehouse authorized by customs authorities for storage of goods on which payment of duties is deferred until the goods are removed.

**BOOKING**: An arrangement with a steamship company for the acceptance and carriage of freight. Generally, the first point of contact between the shipper and carrier. Acts as a reservation to hold space on a vessel.

**BOOT TOPPING:** Technically, the area of a ship's hull between the light and full load waterline. Typically, the paint in the area of the ship's hull, which is alternately immersed and exposed as state of loading changes. The boot topping need not stop at, or near, the LOAD WATERLINE, and the amount of exposed boot topping, alone, cannot provide an accurate measure of the state of ship's loading.

**BROKEN UP:** Said of a ship when it has been reduced to scrap metal. Ships may be removed from service and DISMANTLED but remain in existence as floating storage or in service as barges. Ships sold to be broken up may continue in service for indefinite periods of time. It is very common for a ship to carry a final cargo, often of scrap metal, on its delivery to the breakers.

**BROKER:** An intermediary who negotiates terms for charters, insurance, sales and purchase of ships, and/or generation of cargo. Not normally the owner of a ship nor of the cargo being negotiated.

**BUNKERS:** Fuel consumed by the engines of a ship, or the, compartments in which such fuel is carried.

**BUYER CREDIT**: A credit arrangement established for financing of imported products with the buyer carrying the credit obligation. Recourse is to the buyer and the strength of the credit rests on the credit worthiness of the buyer. Export guarantee and insurance programs from the country are often available to facilitate such transactions.

**CABLE TRANSFER**: A type of remittance using electronic transmission to move funds from one bank to a named party at another bank.

**CAMBER:** Curvature of a deck such that it is highest fore and aft along the centerline and curves downward at the sides. Provides strength and facilitates rue-off of waves.

**CAPTIVE REGISTER:** A REGISTER of ships maintained by a territory, possession, or colony primarily or exclusively for the use of ships owned in the parent country, Also referred to as an OFFSHORE REGISTER, and the "offshore" equivalent of an INTERNAL REGISTER. Ships on a captive register will fly the same flag as the parent country, or a local variant of it, but will be subject to the maritime laws and taxation rules of the offshore territory. Although the nature of a captive register makes it especially desirable for ships owned in the parent country, like the internal register the ships may also be owned abroad. The captive register then acts as a flag of convenience register, except that it is not the register of an independent state.

**CARGO:** Traditionally defined as "freight loaded unto a ship or vehicle," cargo is frequently classified as either containerized or non-containerized. Containerized cargo:

- Includes all goods that can be loaded into a container having the following dimensions: 8' by (8'6" or 9'6") by (20', 40', or 45') and shipped as a full container

- Includes all goods that can be loaded into specialized containers and shipped as a full container

- Includes shipped goods that do not fill an entire container, but are matched with other fractional loads (consolidation), possibly owned by other parties, to move the goods through the transportation system in a full container. Due to the nature of these shipments, the individual shipments are unloaded at a destination and then shipped to their respective consignees. This approach exposes additional risk to these shipments to loss or damage as they no longer have the protection of the container.

- Provides advantages by unitizing cargo, protecting it from weather and the difficulty of shipment, and making it easier to load and unload

- Remains in the same container throughout an cargo transport, since this container can be loaded directly onto maritime and container-ship vessels for water shipments, stacked or "piggybacked" on rail cars for long-haul trips, and moved by tractor trailer to final destinations

Non-containerized cargo includes three categories of shipped goods:

- Bulk cargo can be air-blown, pumped, conveyor-belted, or generally handled in bulk rather than discrete units. Examples include petroleum products, grain, sand,

gravel, dry chemicals, and bulk liquids. Also, other bulk items known as "bagged" cargoes are: peas, beans and lentils.

- Break-bulk cargo, historically referred to as general or packaged cargo, has a high value per unit of weight, is usually manufactured or processed, and moves by number or count. Break-bulk cargo usually moves in smaller quantities than bulk cargo, and originally was loaded or unloaded piece-by-piece. Examples include machinery, yachts, and some wood products, such as newsprint, pulp, and linerboard.

Neo-bulk cargo, though historically classified as general cargo, moves in volume, usually on specialized or dedicated vessels or vehicles. Examples include automobiles, steel, logs, and cattle.

**CARNET**: A customs document permitting the holder to carry or send merchandise temporarily into certain foreign countries (for display, demonstration, or similar purposes) without paying duties or posting bonds.

**CARRIER:** Any person or entity who, in a contract of carriage, undertakes to perform or to procure the performance of carriage by rail, road, sea, air, inland waterway or by a combination of such modes. Also, the issuer of a Bill of Lading (BOL).

**CASH AGAINST DOCUMENTS (CAD)**: Payment for goods in which a commission house or other intermediary transfers title documents to the buyer upon cash payment.

**CASH IN ADVANCE (CIA)**: Payment for goods in which the price is paid in full before a shipment is made. This method is usually used only for small purchases or when goods are built to order.

**CASH WITH ORDER (CWO)**: Payment for goods in which the buyer pays when ordering and in which the transaction is binding on both parties.

**CELLULAR VESSEL:** Ship specially designed and arranged for the carriage of containers. Holds or cells are arranged so that the containers are lowered and stowed in a vertical line and restrained at all four corners by vertical posts. Normally stowed containers sit up to seven high below decks and three to four high above decks.

**CERTIFICATE OF INSPECTION**: A document that notes the condition of the merchandise immediately prior to its shipment.

**CERTIFICATE OF MANUFACTURE:** A statement (often notarized) in which a producer of goods certifies that manufacture has been completed and that the goods are now at the disposal of the buyer.

**CERTIFICATE OF ORIGIN**: A document in which the exporter certifies to the place of origin (manufacture) of the merchandise to be exported. Sometimes these certificates must be legalized by the consul of the country of destination, but more often they may be legalized by a commercial organization, such as a Chamber of Commerce, in the country of manufacture. Such information is primarily to comply with tariff laws.

**CGS** - CONTAINER FREIGHT STATION: A warehouse facility, either on-dock or off-dock, where less-than-containerload (LCL) shipments are consolidated into full container load shipments.

**CHANDLER:** A merchant who supplies ships with stores and provisions.

**CHARTER:** The hiring of a vessel or part of its capacity. Chartering activity is one of the least reported of legitimate maritime operations; most deals being made on a private and confidential basis. Only approximately 50% of charters are ever reported in commercial shipping sources. Charters of less than a full ship (SPACE CHARTER, SLOT CHARTER) are almost never reported.

**CHARTER PARTY:** The basic document between vessel owner and charterer setting forth the type charter, duration, and rates of payment, tonnage, capacity and condition of the vessel course it is to pursue, loading and discharge ports, redelivery port, responsibility for bunkering, insurance, manning, end operations.

**CHARTERED SHIP:** A vessel under lease by its owner to others.

**CHARTERING TERMINOLOGY**: See individual entries for:

- *BAREBOAT CHARTER*
- *CHARTER*
- *CHARTER PARTY*
- *DEMISE CHARTER*
- *PERFORMANCE CLAUSE*
- *RANGE OF PORTS*
- *SLOT CHARTER*
- *SPACE CHARTER*
- *TIME CHARTER*
- *VOYAGE CHARTER*

**CHASSIS:** A trailer constructed to accommodate containers which are moved over-the-road.

**CHIPS**: An acronym for the Clearing House Interbank Payments System, a computer system operated by New York banks to settle international payments. Using CHIPS, checks are cleared, other instruments are exchanged and net balances are settled among banks.

**CLEAN BILL OF LADING**: One in which the goods are described as having been received in "apparent good order and condition" and without qualification.

**CLEAN COLLECTION**: A collection in which a check or draft is present for payment without additional attached documentation.

**CLEAN CREDIT**: A letter of credit payable upon presentation of a draft, not requiring any other payment.

**CLEAN DRAFT**: A draft to which no documents have been attached.

**CLIP ON UNIT:** A piece of refrigeration equipment which can be attached to an insulated (refrigerated) container or hung on the underside of a chassis to supply power to a container which does not have its own self sustaining refrigeration unit.

**COLLECTING BANK**: A bank that acts as an agent for the remitting bank. The collecting bank demands payment from the buyer and handles the funds received as instructed: generally, the funds are sent back to the remitting bank.

**COLLECTION**: A financial transaction in which a bank acts as an intermediary between two parties, (usually a buyer and seller located in different geographic areas), to facilitate the collection of a payment.

**COMMERCIAL ATTACHE:** The commerce expert on the diplomatic staff of his or country's embassy.

**COMMERCIAL BILL**: A bill of exchange drawn by an exporter directly on the importer.

**COMMERCIAL VESSEL:** Any MERCHANT SHIP that is engaged in trading for cargo carrying purposes.

**COMMON CARRIER:** A transportation company operating under a certificate of convenience and necessity for the purpose of providing services to the general public at published rates.

**CONFIRMED LETTER OF CREDIT**: A letter of credit, issued by a foreign bank, the validity of which has been confirmed by a US bank. An exporter whose payment terms are a confirmed letter of credit is assured of payment by the US bank even if the foreign buyer or foreign bank defaults.

**CONSIGNEE**: The party for whom the cargo is destined. The receiver of a CARGO. In a BILL OF LADING, not necessarily the end user.

**CONSIGNOR:** The SHIPPER of a CARGO.

**CONSULAR INVOICE**: A document, required by some foreign countries, describing a shipment of goods and showing information such as the consignor, consignee, and value of the shipment. Certified by a consular official of the foreign country, it is used by the country's customs officials to verify the value, quantity, and nature of the shipment.

**CONTAINER FREIGHT STATION (CFS):** The physical facility where goods are received by carrier for loading into containers or unloading from containers and where carrier may assemble, hold, or store its container or trailers.

**CONTAINER TERMINAL:** An area designated for the stowage of cargoes in container; usually accessible by truck, railroad, and marine transportation. Here containers are picked up, dropped off, maintained, and housed.

**CONTAINER**: A truck trailer body that can be detached from the chassis for loading into a vessel, a rail car, or stacked in a container depot. Containers may be ventilated, insulated, refrigerated, flat rack, vehicle rack, open top, bulk liquid, or equipped with interior devices. A container may be 20 feet, 40 feet, 45 feet, 48 feet, or 53 feet in length, 8'0" or 8'6" in width, and 8'6" or 9'6" in height.

**CORRESPONDENT BANK**: A bank that, in its own country, handles business of a foreign bank.

**COST AND FREIGHT (CFR)**: A shipping term under which the seller quotes a price including the cost of transportation to the named point of destination.

**COST INSURANCE AND FREIGHT (CIF)**: A shipping term under which the seller quotes a price including the cost of goods, the marine insurance, and all transportation charges to the named point of destination. Commonly used commercial practice, especially for import to Third World countries, The cost of cargo includes the costs of transportation and insurance to the delivery port. A ship involved in a CIF delivery will thus normally be on charter to, or under the control of, the exporter. Although the CIF method involves higher cost, the importer need not charter a ship or deal with the myriad of brokers involved in moving and insuring a cargo, and his risk begins only when the cargo leaves the ship, over which he exercises no control.

**COUNTRY RISK**: Financial risk base on the evaluation of political, economic, and social conditions of a country.

**CREW LEASING:** A term which probably describes the managerial function of agreeing to supply an entire "turnkey" crew for a given ship. This term would imply that the crewing management firm which gathered, and certified as competent such a crew, would probably pay them, while collecting its fee from the owner/operator, In this case,

then, the crew would work for the crewing manager and not for the ship owner or charterer.

**CUBED OUT:** Said of a ship when it is full by volume without being loaded down to its LOAD LINE and not carrying the full DEADWEIGHT TONNAGE to which it is entitled.

**CUSTOMS INVOICE:** A document that contains a declaration by the seller, the shipper, or the agent of either as to the value of the goods covered.

**CONTAINER YARD (CY):** Point forest for a container. This can be a part of the terminal where vessels are loaded or can be an "off dock" facility which is not apart of the terminal loading area.

**DEADWEIGHT TONNAGE (DWT):** The total carrying capacity of a ship in metric tons. This figure includes the weight of fuel and stores as well as cargo. Current rules of thumb for estimating cargo capacity of a ship (cargo deadweight) are: 95% of deadweight for large tankers and 85& of deadweight for dry cargo/container ships. Smaller, older ships will have lower cargo deadweight as a result of less efficiency in design and higher bunker requirements to support less efficient engines. When military cargo is being carried it is normal for a ship to sail partially loaded, or for the ship to be full by volume before it reaches its limit in weight. The ship is then said to be CUBED OUT. This is partly due to the nature of much military equipment which will not permit stacking, leading to waste of volume.

**DECLARATION:** Statement from a ship on leaving port or passing a reporting station as to its next port of call. Ultimate ports of call can be given and intermediate ports omitted and the presence of a declaration is not, of itself, proof of where a ship intends to proceed. When used legitimately, the declaration that a ship is bound for a given port "for orders" or "AWAITING ORDERS" indicates that the ship is not carrying cargo beyond that port.

**DEMISE CHARTER:** See BAREBOAT CHARTER

**DISMANTLED:** Normally and accurately used to describe the removal of a ship's engines or otherwise having been rendered incapable of self-propelled navigation. Can also be less accurately used interchangeably with SCRAPPED or BROKEN UP.

**DISPOSAL:** Normally the deletion from a fleet or group of ships (such as a company) of an individual ship or group of ships. Ships sold to be BROKEN UP or sold to another registered owner/operator would be referred to as disposed of by the loosing firm. Ships for which charter arrangements are terminated will leave the fleet of a given operator or a service. They would not normally be referred to as having been disposed of, however. A ship may be listed by an owner as "for disposal" when it has been designated as being for sale. The ship can continue to operate or can be laid up, at the owner/operator's

discretion, while awaiting the disposal. Ships listed for disposal for scrapping often continue to exist for long periods of time without operating while the owner waits for scrap prices and other conditions to be favorable.

**DATE DRAFT**: A draft that matures in a specified number of days after the date that it is issued, without regard to the date of acceptance.

**DEPOT**: Locations where empty containers are held in storage.

**DISHONOR:** The refusal of a drawee to accept a draft or pay for it when due.

**DOCK RECEIPT**: A receipt issued by an ocean carrier to acknowledge receipt of a shipment at the carrier's dock or warehouse facilities.

**DOCUMENTARY COLLECTION**: A collection in which a draft is accompanied by shipping or other documents.

**DOCUMENTARY CREDIT:** A letter of credit that requires documents to accompany that draft of demand for payment.

**DOCUMENTARY DRAFT**: A draft to which documents are attached

**DOCUMENTS:** Items presented along with the draft. These may include the bill of lading, the commercial invoice, the marine insurance policy or certificate of origin, the weight list, the packing list, and the inspection certificate (or certificate of analysis). Under a letter of credit, the documents must be examined for compliance before the draft is paid.

**DOCUMENTS AGAINST ACCEPTANCE (D/A):** Instructions given by a shipper to a bank indicating that documents transferring title to goods should be delivered to the buyer (or drawee) only upon the buyer's acceptance of the attached draft.

**DOCUMENTS AGAINST PAYMENT (D/P** - Draft: A sight or time draft to which documents are attached. The documents are surrendered to the drawee only when the drawee has paid the corresponding draft.

**DRAFT (BILL OF EXCHANGE):** An instrument, much like an ordinary check in appearance, which is used as a formal demand for payment in a business transaction.

**DRAWEE:** The individual or firm on whom a draft is drawn and who owes the stated amount.

**DRAWER**: The issuer or signer of a draft.

**DRAWING:** Presentation of the draft and documents required by the terms of a letter of credit.

**DRAYAGE:** Trucking which is performed to/from the shipper's location to an interchange point inland or to/from a container yard. Drayage is usually performed by the shipper's trucker, or the carrier's contract trucker.

**EDI**: Electronic Data Interchange.

**ENDORSEMENT:** A signature on the back of a negotiable instrument made primarily for the purpose of transferring the rights of the holder to some other party. It is a contract between the holder and all parties to the instrument.

**EQUIPMENT INTERCHANGE RECEIPT (E.I.R.):** A form used by the parties delivering or receiving containers and container equipment. It is used for equipment control and damage purposes-Synonymous with T.I.R (TRAILER INTERCHANGE RECEIPT).

**EXPORT BROKER:** An individual or firm that brings together buyers and sellers for a fee but does not take part in actual sales transactions.

**F.A.K.:** Freight all kind.

**F.C.L.:** Full container load. The maximum permissible weight for the value of the cargo carried in a container.

**FEEDER SERVICE:** Coastal movements of loaded/empty containers on board smaller container vessels which coordinate with a mother ship for the ocean voyage.

**FEU:** Forty-foot equivalent unit. Term indicating capacity of container vessel or terminal.

**FLAG OF CONVENIENCE REGISTER:** A national register offering registration to a merchant ship not owned in the FLAG STATE, The major flags of convenience (FOC) attract ships to their register by virtue of low fees, low or non-existent taxation of profits, and liberal manning requirements. True FOC registers are characterized by having relatively few of the ships registered actually owned in the flag state. Thus, while virtually any flag can be used for ships under a given set of circumstances, a FOC register is one where the majority of the merchant fleet is owned abroad. Also referred to as an OPEN REGISTER.

**FLAG STATE:** The nation in which a ship is registered and which holds legal jurisdiction as regards to operation of the ship, whether at home or abroad. Differences in Flag State maritime legislation determines how a ship is manned and taxed, and whether a foreign owned ship may be placed on the register.

**FOREIGN DRAFT:** A draft drawn by a bank on a foreign correspondent bank and sent to the payee.

**FOUL BILL OF LADING:** A receipt for goods issued by a carrier with an indication that the goods were damaged when received.

**FREE ALONGSIDE (F.A.S.):** A shipping term under which the seller quotes a price including delivery of the goods alongside the vessel and within reach of its loading tackle.

**FREE ON BOARD (FOB):** The term used when the buyer of the goods being shipped assumes ownership, responsibility, and financial risk when the cargo is on board the ship (legally, when it passes over the ship's rail.) A ship on charter to carry a cargo on a FOB basis will therefore, normally, be on charter to the purchaser of the cargo, and not the exporter. This is typically the method used in Third World countries to generate payments quickly (when the cargo is loaded) and to avoid the financial risk associated with having to deliver the cargo to its destination.

**FREEBOARD:** Vertical measurement taken amidships from the Load Waterline, or LOADLINE, to the underside of the FREEBOARD DECK.

**FREEBOARD DECK:** Uppermost watertight deck or deck having weather openings capable of being hermetically sealed.

**FREIGHT:** Transportation charges for CARGO carried by a ship.

**FREIGHT FORWARDER:** A carrier that collects small shipments from shippers, consolidates the small shipments and uses a basic mode to transport these consolidated shipment to a destination where the freight forwarder delivers the shipment to the consignee. A person whose business is to act as an agent on behalf of the shipper. A freight forwarder frequently makes the booking reservation. An independent business that handles export shipments for compensation

**GROSS TONNAGE (GRT):** A statutory measure of permanently enclosed volume in a merchant ship. Originally 100 cubic feet of space equaled one gross ton, and there has never been a way to convert GRT to weight of ship or cargo. A 1969 convention resulted in international agreement on a formula yielding a pure number that relates neither to space nor to weight. The convention also eliminated a situation in which differences in national rules resulted in sometimes-radical changes in a ship's GRT when it changed flag. The GRT, and numbers derived from it, such as Net Registered Tonnage (NRT), form the basis for national registration fees and port and canal dues. While it gives a good approximation of relative size of two ships of the same type, it is a misleading measure of carrying capacity. When cited in reports, GRT is most useful as a means of differentiating a ship from other possible ships of the same name.

**HOG, HOGGING:** A ship is said to be hogged when the ends of the ship are depressed below the center. This may result from improper cargo stowage, with too much weight at the ends. It is a naturally occurring tendency when a ship is suspended at the crest of a wave with each end relatively unsupported. May cause strain and buckling of hull plates, and in extreme cases, breaking in two. A ship without SHEER will give the impression of being hogged.

**HOUSE CARRIER:** A trucking company that has a contractual relationship with a carrier.

**IDLE:** A merchant ship may be idle between periods of employment carrying cargo. Nevertheless, the ship will be fully provisioned and manned, as opposed to when it is in a LAYUP status.

**IMO NUMBER:** A seven-digit number allotted to every merchant ship hull which is its internationally recognized identity number, introduced by International Maritime Organization (IMO) resolution to assist registration and combat fraud. For ships of all Flags and registries this is the same as the Lloyd's Register Number or LRN.

**INLAND BILL OF LADING:** A bill of lading used in transporting goods overland to the exporter's or from the importer's international carrier. A through bill of lading is many times substituted for an inland one.

**INLAND CARRIER:** A transportation line that hauls export or import traffic between ports and inland points.

**INTERMODAL:** Used to denote movements of cargo containers interchangeable between transport modes, i.e. motor, water, and air carriers, and where the equipment is compatible within the multiple systems.

**INTERMODAL TRANSPORT:** The capability of interchange of freight containers among the various transportation modes. The fact that the containers are of the same size, and have common handling characteristics, permits them to be transferred from truck to railroad to air carrier to ocean carrier, in a complete origin-to-destination movement.

**INTERNAL REGISTER:** A register of ships maintained as a subset of a national register. Ships on the internal register fly the national flag and have that nationality, but are subject to a separate set of maritime rules from those on the main national register. These differences may include lower taxation of profits, manning by foreign nationals, and ownership outside the flag state (when it functions as a flag of convenience register), The Norwegian International Ship Register and Danish International Ship Register are the most notable examples of an internal register. Both have been instrumental in stemming flight from the national flag to flags of convenience and, to an extent, in attracting foreign owned ships to the Norwegian and Danish flags.

**IRREVOCABLE LETTER OF CREDIT:** A letter of credit in which the specified

payment is guaranteed by the bank if all terms and conditions are met by the drawee.

**INSPECTION CERTIFICATE:** A certificate usually issued by an independent third party when inspection is called for in the merchandise contract.

**JOINT VENTURE**: A venture or business activity undertaken by two or more people or firms in a merger or partnership, For purposes of maritime joint ventures, the individual ships participating need not be jointly owned, but rather could be contributed to a joint service. Management and operation of ships in a joint venture could be by the original owner(s), by the joint venture company, or by a third party manager hired for this purpose. None of these arrangements would affect ownership, per se, and would not therefore be subject to our routine scrutiny

**LAYUP**: An idle merchant ship will be placed in layup when no immediate employment seems in prospect. Layup will normally involve partial preservation of engineering spaces and removal of all or most of the crew. A laid up ship cannot, therefore, be immediately reactivated. This is different from the case of a ship being DISMANTLED which renders the ship incapable of reactivation without installation of propulsion equipment.

**LEASE :** Not correctly used as the equivalent of CHARTER. A ship may be leased to an operator by the PARENT COMPANY which is not a ship operator. For example, banks frequently become the owners of ships, either intentionally as part of a speculative new building, or unintentionally as part of a repossession. The effect of a lease arrangement will be essentially the same as that of a BAREBOAT CHARTER.

**LEGAL TERMINOLOGY** - See individual entries for:

- *ARREST*
- *FLAG STATE*
- *LIEN*
- *NATIONALITY*
- *REGISTER*
- *SEIZURE*

**LETTER OF CREDIT:** An instrument, issued by a bank upon request by a customer, that states the bank will pay an obligation of its customer's to a third party when certain stated conditions have been met. The two most frequently used letters of credit are the commercial letter of credit, which is used to finance the buying and selling of merchandise, and the standby letter of credit, which is used to support a customer's obligations to perform under a contract. An international business document that assures the seller that payment will be made by the bank issuing the letter of credit upon fulfillment of the sales agreement.

**LIEN:** A legal right by which a person (or company) is entitled to obtain satisfaction of a debt by means of property belonging to the person indebted to him. Maritime liens attach to a ship, its cargo, or the payments received or pending, and are normally enforced by ordering the ARREST of the ship or its cargo.

**LIGHTERING:** The discharge or, more rarely, loading of cargo while at anchor. This is done where port facilities are inadequate, where a port is overcrowded, or where several small cargoes are being consolidated into one. This operation is most common with tankers or with bulk carriers carrying grain, and least common with container ships and roll-on/roll-off ships.

**LINE:** Although often used interchangeably with ship OWNER, the term line correctly refers to a service, usually of regularly scheduled ships over an advertised route. The ships need not, and often do not belong to a single owner.

**LINE OF CREDIT**: A commitment by a bank to a borrower to extend a maximum amount of credit in a series of transactions. A line of credit, acceptance and/or discounting of drafts, multiple loans of drafts, multiple loans of advances and other forms of credit.

**LLOYD'S REGISTRY NUMBER (LRN):** See IMO NUMBER.

**LOAD LINE:** The mark permanently inscribed and painted on the side of a ship, amidships, which designates the greatest depth to which it can be legally loaded. The mark consists of a circle bisected by a horizontal bar. When the circle is half submerged the ship is at its full DEADWEIGHT capacity. Also known as the Plimsoll Mark. The painted BOOT TOPPING of a merchant ship hull does not have to stop at the load WATERLINE and may continue beyond or stop short. The only reliable indicator of whether a ship is loaded or in BALLAST is the relation of the load line to the waterline.

**MAIN DECK:** The uppermost continuous deck of a ship, running fore to aft. Normally, the FREEBOARD DECK.

**MANAGER:** A company which specifically manages (crews, operates, finds cargo for, insures, performs accounting functions for, etc.) a ship or group of ships. May also, in fact own the ships, either as a registered owner or as a parent company (MANAGING OWNER), The manager and charterer, if any, exercise more day-to-day operational control over a ship than does the registered owner or parent company, under normal circumstances.

**MANAGING OWNER:** One, usually of several co-owners, to whom the others have delegated management of the ship or ships. The term managing owner at least implies that the ship is owned by more than one firm or set of partners.

**MANIFEST:** A full list of a ships cargo, extracted from BILLS OF LADING. A copy, known as the outward manifest, is lodged with the customs authorities at the port of loading, Another, the inward manifest, is lodged at the discharge port, with a copy for the ship's agent (now frequently transmitted electronically) so that unloading may be planned in advance.

**MERCHANT MARINE:** All ships engaged in the carriage of goods. All commercial vessels (as opposed to all non-military ships) which excludes tugs, fishing vessels, offshore oil, etc. Also, a grouping of MERCHANT SHIPS by NATIONALITY or REGISTER.

**MERCHANT SHIP:** A vessel that carries goods against payment of FREIGHT. Commonly used to denote any non-military ship, but accurately restricted to commercial vessels, only.

**NATIONALITY:** For a ship this is provided by the flag flown as a result of having been legally entered onto the REGISTER of a country which maintains such a shipping register. All legal jurisdictions over the ship resides with the flag state which grants nationality to the ship, regardless of the nationality or location of the vessels actual owner.

**NEGOTIABLE INSTRUMENT:** Any written evidence of an obligation which may be transferred by Endorsement or by delivery, and of which the transferee may become a holder in due course. Examples include: checks, bills of exchange, drafts, promissory notes and some types of bonds or securities

**NEGOTIABLE LETTER OF CREDIT:** The letter of credit which allows the beneficiary to present the documents and draft to a named bank (the nominated bank) or to any bank willing to negotiate them on or before the expiration date.

**NEGOTIATE (LETTER OF CREDIT):** Giving of value for draft(s) and/or document(s) by the bank authorized to negotiate.

**NON-VESSEL-OWNING COMMON CARRIER (NVOCC):** A firm that consolidates and disperses international containers that originate at or are bound for inland ports.

**OPEN ACCOUNT (O/A)**: Open account, no draft drawn. Transaction payable when specified, i.e., RJM: return mail, E.O.M. - end of month; 30 days – 30 days from date of invoice, 2/10/60 - 2% discount for payment in 10days, net if paid 60 days from date of invoice. If no term is specified, O/A usually implies payment by return mail.

**OPENING BANK:** The bank that issues the letter of credit and that makes payment according to the conditions stipulated (also known as Issuing Bank).

**OPEN REGISTER:** See FLAG OF CONVENIENCE REGISTER.

**ORDER BILL OF LADING:** Usually, "To Order" bills of lading are to the order of the shipper and endorsed in blank, thereby giving the holder of the B/L title to the shipment.

They may also be to the order of the consignee or bank financing the transaction. Order Bills of Lading are negotiable (whereas Straight Bills of Lading are not).

**OWNER-** (see also MANAGING OWNER, REGISTERED OWNER, PARENT COMPANY), Ambiguous term, which can mean either the registered owner or the parent company which actually controls such matters as the purchase and disposal of the ship. In all cases, the owner is the individual or firm with financial equity or which is considered to be at risk if the ship is lost or libeled. In practical terms, the owner would be the beneficiary of any insurance policy on the ship, but we are rarely in a position to know who those entities are. Owner of ships need not be firms or individuals, at all, but can be countries or ministries of countries. Thus, the REGISTERED OWNER of a Cuban flag-of-convenience ship could be Rose Islands Steamship Company. The PARENT COMPANY might then be Empresa Mambisa. The true OWNER is the Government of Cuba because it owns Mambisa, which owns Rose Islands.

**PACKING LIST:** A list prepared by the manufacturer, detailing the particulars of the merchandise to be sold, including the containers in which the goods are packed, their contents, and the total number of containers.

**PARENT COMPANY** (also referred to, somewhat inaccurately, as BENEFICIAL OWNER)
The ultimate ship-owning level in a string of firms, the lowest of which owns individual ships. Thus, properly used, a PARENT COMPANY owns other companies. The parent company may be owned by larger conglomerates which have shipping as subsidiary interests, or by the Government of Countries.

**PERFORMANCE BOND:** A bond issued at the request of contractors to support their commitment to perform under contract.

**PERFORMANCE CLAUSE:** Part of the TIME CHARTER party specifying performance the ship shall be able to attain. If the ship is too slow, or burns too much fuel, the charterer is entitled to recover the cost of time lost or excess fuel consumed.

**PIRACY:** An assault on a vessel, cargo, passengers, or crew, usually from another vessel while at sea by persons acting for personal gain and not acting on behalf of any recognized flag or International authority. Also includes acts of rioters who attack a ship from the shore for the purpose of theft or of passengers who attack the ship and its personnel from on board.

**PRO FORMA INVOICE:** An invoice provided by a supplier prior to the shipment of merchandise, informing the buyer of the kinds and quantities of goods to be sent, their value, and important specifications.

**PROVISIONS:** Food and beverages supplied to a ship for its crew and passengers. Included in the meaning of STORES.

**RAILBILL OF LADING:** A document exchanged between a shipper or shipper's agent and a railroad, which describes the required movement of a container via rail.

**RANGE OF PORTS:** A series of ports at which a charter party will permit a ship to discharge, one of which is to be nominated by the charterer by a specific date. Generally expressed by the names of the ports at either end of the range, e. g. the Hamburg Antwerp range. The ship will frequently be underway before the discharge port is known, and could appear to be describing an erratic track or to have given a false DECLARATION as a result.

**RE-CONSIGNMENT:** The act of changing the Bill of Lading as to consignee or destination, while the shipment is in transit.

**REEFER CONTAINER-** Refrigerated container.

**RE-FLAG:** To transfer the registry of an existing, registered, ship from one national authority to another. The normal procedure is to first "sell" the ships to a new REGISTERED OWNER under the jurisdiction of the country to which the ship is being re-flagged. That new registered owner then registers the ship under the new flag and may, or may not, depending on the requirements of the maritime laws of the countries involved, terminate the old register. At the most basic legal level, re-flagging changes the set of national laws and jurisdictions under which the ship operates. Under international law and practice the ship has the nationality of the political entity whose flag it is entitled to fly. Suits brought against the owner of the ship, for non-payment of mortgages, etc., have to be in accordance with the law of the flag state.

**REGISTER:** The record of a ship's ownership and nationality as listed with the maritime authorities of a country. Also, the compendium of such individual ships, registrations within a country. Registration of a ship provides it with a nationality and makes it subject to the laws of the country in which registered (the FLAG STATE) regardless of the nationality of the ship's ultimate owner.

**REGISTERED OWNER:** The owner of record of an individual ship that is listed on the registration documents (filed with a national authority).

**REGISTRATION TERMINOLOGY:** see individual entries for:

*CAPTIVE REGISTER*
*FLAG OF CONVENIENCE REGISTER*
*FLAG STATE*
*INTERNAL REGISTER*
*NATIONALITY*

**REMITTANCE:** A transfer of funds from one place to another.

**REMITTING BANK:** The bank that sends the draft to the overseas bank for collection.

**REVOCABLE LETTER OF CREDIT:** A letter of credit that can be canceled or altered by the drawee (buyer) after it has been issued by the drawee's bank.

**REVOLVING LETTER OF CREDIT:** A letter of credit that provides for specified payments on shipments of goods that take place on a regular basis over a period of time. A revolving letter of credit may be issued on a revolving-by-amendment basis or an automatic revolving basis.

**SAG, SAGGING:** A ship sags when its fore and aft ends are bent upward. This can be caused when there is too much weight in the center of the ship, or when its weight is supported at the ends, and not in the middle. This occurs naturally when bow and stern are in a wave, but the amidship section is in a trough. The upper deck edge of a ship may appear to be sagging due to the ship's SHEER, or lack of it, but it is the shape along the concealed keel that governs use of the term.

**SALE:** Change of owner of a ship corresponding to an agreement which usually involves transfer of funds. The actual, transfer of funds could be "on paper" only, and the only change of owner required to generate a typical sale report would be that of the REGISTERED OWNER, Since a sale does not automatically result in a change of manager or charterer, it does not automatically follow that a sale will result in a shift of control of a ship.

**SEIZURE:** In marine law includes capture or seizure by revenue customs officers of a foreign state and covers every act of taking possession of a ship. The word seizure has a stronger meaning than ARREST as it may be interpreted to be a forcible possession by an overpowering force or authority of the state.

**SHEER:** The upward curve of a deck and lines of a ship from amidships toward bow and/or stern. A convex curve, whereas the camber will be concave.

**SHIPPER:** Person offering the goods for transportation. A person or company which engages ship owners or operators to carry cargo.

**SHIP'S MANIFEST:** An instrument in writing, signed by the captain of a ship, that lists the individual shipments constituting the ship's cargo.

**SIGHT CREDIT:** A letter of credit under which drafts are payable upon presentation or on demand if the documents meet the terms and conditions of the letter of credit.

**SIGHT DRAFT (S/D)**: A draft so drawn as to be payable on presentation to the drawee (or within a brief period thereafter, known as "days of grace"); also referred to as a Demand draft. Custom, in certain areas, has in effect made an Arrival Draft out of a Sight Draft because buyers often will pay a Sight Draft until the arrival of the carrying vessel.

**SLOT CHARTER:** Typically used to denote hiring of space (slots) aboard a container ship by a shipper who can generate a fixed amount of cargo but one insufficient to justify taking an entire ship on hire. This type of charter will not give the charterer any control over the movement and employment of the ship. Also, less typically, used to designate a specific voyage charter to replace a temporarily unavailable ship.

**SPACE CHARTER:** The taking on hire of part of ship's capacity. Unlike a SLOT CHARTER, the space charter does not necessarily imply a long-term relationship. This type of charter will not give the charterer any actual control over the employment and movement of the ship.

**STALE BILL OF LADING:** A bill of lading which is not presented to the bank within the time frames specified in the letter of credit. Or, if no date is specified, within 21 days following the date of shipment in accordance with UCP 500.

**STANDARD INTERNATIONAL TRADE CLASSIFICATION (SITC):** A standard numerical code used to classify commodities used in international trade.

**STANDBY LETTER OF CREDIT:** A letter of credit issued at the request of the bank's customer ensuring payment by the bank to the beneficiary in the event the customer does not fulfill the underlying obligation and the beneficiary complies with the terms of the letter of credit.

**STIFF:** Said of a ship having a tendency to roll quickly or with a "snap" roll. Normally caused by stowage of heavy or dense material low in the ship.

**STORAGE VESSEL or STATION VESSEL:** A merchant ship that is in use at a port to consolidate part cargoes for transfer to similar or larger ships. A storage ship can normally also get underway to carry cargo if so desired, but usually acts in a stationary capacity over a long period. Can function as a spare parts warehouse for visiting ships in addition to its primary function providing cargo storage, Provides a stationary function similar to the mobile one of LIGHTERING.

**STORES:** Supply of fresh and dry provision and the supplies for the running of the ship, such as lubricating oil, line, and spare parts.

**STOWAGE FACTOR:** The ratio of a cargo's cubic measurement to its weight, expressed in cubic feet/meters to the ton. Used in conjunction with the GRAIN or BALE capacities to determine how much total cargo may be loaded.

**STOWAGE PLAN:** A plan in the form of a longitudinal cross-section of the ship, which shows the location in the ship' of all consignments of cargo, frequently color coded to highlight the various ports of discharge. The stowage plan is used by the Chief Mate (or First Mate) who draws it up to plan discharging of the cargo. In modern container ships the stowage plan will be a computerized document, normally prepared ashore by the ships operations office.

**STRAIGHT BILL OF LADING:** A nonnegotiable bill of lading in which the goods are consigned directly to a named consignee.

**STRIPPING:** A term often used to denote the process for removing cargo from a container.

**STUFFING:** Denotes the process of loading cargo into a container.

**SUPERCARGO:** A person employed by a ship owner, charterer of a ship, or shipper of goods to supervise cargo handling operations and/or the security of the cargo in transit, During Desert Shield/Storm military personnel often accompanied shipments of weapons and ammunition to the Kuwait Theater of Operations.

**S.W.I.F.T.**: An acronym for Society for Worldwide Interbank Financial Telecommunications. This international system has been established to move funds and information more efficiently among member banks.

**TARIFF**- A customs charge on imported goods. In reality, tariffs are a form of tax.The back-to-back letter of credit is generally used in international trade when the exporter, a) is not the supplier, b) does not have ready funds to pay the supplier, and c) does not want the supplier to know the price of the goods or the name of the importer. It is an extension of the terms and conditions of the backing credit. The party instructing the bank to open a letter of credit on whose behalf the bank agrees to make payment. In most cases, the account party is an importer or buyer, but may also be a construction contractor or a supplier bidding on a contract.

**TENDER:** Said of a ship with a tendency to roll slowly, or to hang on the outer edges of a roll. Normally caused by stowage of heavy or dense material high up in the ship. Although a tender ship has a more comfortable roll than one that is stiff, it is the stiff ship, which has the greatest stability, as demonstrated in its ability to right itself.

**TEU:** Twenty-foot equivalent unit. The common unit used indicating capacity of a container vessel or terminal.

**THROUGH BILL OF LADING:** A single bill of lading converting both the domestic and international carriage of an export shipment.

**TIME CHARTER:** Hire of a ship and its crew for a set period. Subject to any restrictions within the CHARTER PARTY the charterer will determine what cargo will be carried, and to which ports. The charterer is responsible for the ship's bunkers, payment o cargo handling and port charges. The owner continues to pay the crew, and hull and machinery insurance and remains responsible for the navigation and technical operation of the ship.

**TIME DRAFT:** A draft maturing at a certain fixed time after presentation or acceptance. Maturity may be a given number of days after sight (acceptance) or a given number of days after date of draft.

**TRADE ACCEPTANCE:** A draft drawn by the seller of goods on the buyer and accepted by the buyer. It often includes a statement indicating that the acceptor's obligation arises out of the purchase of goods from the drawer of the draft.

**TRANSACTION STATEMENT:** A document that delineates the terms and conditions agreed upon between the importer and exporter

**TRANSFERABLE LETTER OF CREDIT:** A letter of credit addressed to the beneficiary "and/or transferee (or transferees)," enabling the beneficiary to transfer the credit to another party.

**TRANSSHIP:** To transfer goods from one transportation line to another or to transfer goods from one vessel to another.

**TRANSSHIPMENT:** A term used when shipment to a destination is best reached by reshipping the goods from another port.

**TRIM (1):** The relationship between a ship's draught forward and aft. If a ship cannot be maintained level on an even keel it is safer to trim the ship down slightly by the stern. This serves to keep waves from breaking over the forepart of the ship, and more fully submerges the propeller and rudder, increasing their effectiveness. The term "trimmed by the bow (or head)" and "trimmed by the stern" mean that the bow or stern are lower in the water, respectively.

**TRIM (2):** To move cargo or adjust ballast to affect the ships trim. To level a bulk cargo in a ship's hold to maximize its stability while at sea.

**UNCLEAN BILL OF LADING:** One in which a notation has been made by the carrier of any defects found in the goods when they are received for transporting. For example, such phrases as "3 hogsheads broken" or "4 sacks torn" may be inserted.

**UNIFORM CUSTOMS AND PRACTICE FOR DOCUMENTARY CREDITS:** The rules and guidelines agreed to by representatives of the private sector engaged in international trade, for the conduct of trade covered by letters of credit. Generated under the sponsorship of the International Chamber of Commerce, the rules have been published as the "Uniform Customs and Practice for Documentary Credits (1993 Revision) International Chamber of Commerce Publication No. 500." The effective date is January 1, 1994.

**USANCE (TIME) CREDIT:** A letter of credit that calls for payment against drafts at some specified date in the future. Usance letters of credit allow buyers payment terms of a specified number of days usually not longer than six months.

**VOYAGE CHARTER:** Contract of carriage for use of a ship (or part of a ship's capacity) for one or more consecutive voyages here the shipowner remains in full control of the ship agreeing to carry a set cargo from a port, or area, to a port, area, or range of delivery ports. The shipowner pays all costs, while collecting from the charterer a fee based on tonnage carried, or a lump sum irrespective of the amount of the ships capacity used. This form of charter leaves maximum control of the ship in the hands of its owner, as opposed to the BAREBOAT CHARTER, which transfers all essential control to the charterer.

**WAREHOUSE RECEIPTS**: In general, a receipt for commodities deposited with a bonafide warehouseman which identifies the commodities deposited. A warehouse receipt on which it is stated that the commodities referred to thereon will be delivered to the depositor or to any other specified person or company is a non-negotiable warehouse receipt; a warehouse receipt on which it is stated that the commodities will be delivered to the "bearer" or to the order of any specified person or company is a negotiable warehouse receipt. Endorsement (without endorsement if issued to the order of "Bearer") and delivery of a negotiable warehouse receipt serves to transfer the property covered by the receipt. There is no difference between a warehouse receipt and a bill of lading in this respect.

**WAYBILL:** A document prepared by a transportation line at the point of origin of a shipment, showing the point of origin, destination, route, consignor, consignee, description of shipment, and amount charged.

**WEATHER DECK:** Uppermost continuous deck of a ship; does not include forecastle, superstructures, or poop. Not necessarily the MAIN or FREEBOARD DECK.

**WEIGHT LIST:** A list showing the weights of either individual parcels, bales or, in the case of bulk commodities, an entire cargo.

**WITHOUT RECOURSE:** A phrase followed by the signature of a drawer or endorser of a negotiable instrument, including a bill of lading, where the signer disclaims liability to subsequent holders in the event of non-payment or non-delivery. Nonetheless, such an endorsement constitutes certain warranties such as the genuineness of the instrument, and the endorser cannot waive liability if any prior signature is proved to be a forgery.

**WITHOUT RESERVE**: A term indicating that a shipper's agent or representative is empowered to make definitive decisions and adjustments abroad.