Supply Chain Security Best Practices Catalog

Customs-Trade Partnership Against Terrorism (C-TPAT)

U.S. Customs and Border Protection

CONTENTS

CONTENTS

PROLOGUE

The Customs-Trade Partnership Against Terrorism (C-TPAT) is, beyond question, the largest and most successful government-private sector partnership to emerge from the terrorist attacks on September 11, 2001. C-TPAT was launched in November 2001, with just seven companies—seven major importers who embraced the necessity of supply chain security within the highest corporate management levels of their organizations. Today, more than 10,000 companies—critical players in the global supply chain—have applied for membership, and more than 6,000 have been accepted as certified partners.

Since the beginning, the guiding principles for C-TPAT have been voluntary participation and jointly developed security criteria, best practices and implementation procedures. C-TPAT partners have worked cooperatively with U.S. Customs and Border Protection (CBP) to protect their supply chains from concealment of terrorist weapons, including weapons of mass effect, and global supply chains are more secure today as a result of C-TPAT. In exchange, CBP provides reduced inspections at the port of arrival, expedited processing at the border, and other significant benefits, such as "front of line" inspections and penalty mitigation. Additionally, C-TPAT status is one variable factored into post-incident contingency planning should a terrorist act impact international supply chains. The security commitment demonstrated by C-TPAT members is strong and meaningful, as are the benefits provided by CBP.

U.S. Customs and Border Protection would like to recognize and thank its many partners in the trade community who have embraced the goals and objectives of the C-TPAT program to improve supply chain security worldwide.

Introduction

This catalog of Supply Chain Security Best Practices (Best Practices) is organized based on the Customs Trade Partnership Against Terrorism (C-TPAT) Security Criteria. The best practices included herein are those that have been identified through more than 1,400 validations and site visits conducted by C-TPAT Supply Chain Security Specialists (SCSS). "Best Practices" are defined as:

1) Security measures that exceed the C-TPAT Security Criteria,
2) incorporate management support,
3) have written policies and procedures that govern their use,
4) employs a system of checks and balances, and
5) have measures in place to ensure continuity.

This catalog is not exhaustive or all-inclusive of best practices in the international supply chain. It is intended to serve as a living document and will be updated periodically to reflect the best practices found during validations.

Best practices are achieved through the effective utilization of people, processes and technology. Best practices incorporate a system of checks and balances, oversight, accountability, and verification of reliability throughout each aspect of the supply chain in order to ensure that the supply chain cannot be compromised. While many of the best practices listed in this catalog may assist businesses in theft prevention and asset protection, their intended use focuses on the prevention of weapons of mass effect, terrorists, or other contraband from entering the supply chain. A single best practice does not constitute an effective supply chain security program. Security best practices must be applied to appropriately reduce the level of risk associated with any international supply chain. It is of paramount importance to approach the international supply chain in its totality, because a chain is only as strong as its weakest link.

In order for a supply chain security best practice to exist, continue to thrive and be effective, they must have the full support of high-level company management. Security best practices should become an integral part of a company's culture by being incorporated into the company's mission and core business processes. Through the validation process, CBP has found that those businesses whose core philosophy is "continuous improvement" have achieved effective supply chain security and have realized many collateral benefits from analyzing the security of their supply chains. Such benefits include but are not limited to development of standards, elimination of duplicative processes to increase efficiency, and greater supply chain visibility. Most importantly, these companies have made significant contributions to global supply chain security by continually improving their security practices.

CBP recognizes the diverse size and financial abilities of C-TPAT members, and this catalog attempts to provide examples of not only advanced security technologies, but of lower cost security practices as well, both of which may help achieve the same security goals. For example, concerning "conveyance tracking," the intended purpose of accurately tracking conveyance movements and detect deviations can be achieved through the use of GPS tracking systems, or through

a lower cost security practice of requiring drivers to follow designated routes with predetermined average travel times, along with periodic communication between the truck driver and company officials. Both of these security best practices help achieve the security goal of conveyance tracking thus providing a more secure environment.

Using this Catalog

This catalog is written in a generic manner to allow for flexibility, maintaining the confidentiality of C-TPAT partners and preventing the endorsement of specific technology, services, or products. Generic business entity names are used (e.g., Company, Logistics Provider, Consolidator, Highway Carrier, Port, Terminal Operator, Sea Carrier, and Air Carrier) in order to provide the context in which the best practice was identified. It is important to note that the best practices listed for these entity types are not necessarily exclusive to the entity mentioned. These best practices are applicable to many industries where the process is performed within the supply chain. For example, a best practice for seal control may be listed as being performed by a consolidator, but a factory may be able to use the same best practice, given that seal control also applies to factories. Generic terms referring to time such as "routinely," "randomly," "intervals," "specified period of time," and "periodically" are meant to convey that a definitive time frame should be established for that best practice.

The *Best Practices Catalog* is not designed as a master check list of security practices which must be adopted in order to receive Tier Three Benefits. The C-TPAT program from its inception has taken a flexible approach, where it is recognized that "one size does not fit all," and that customized security measures must be developed and implemented in accordance with the risk present. For example, the adoption of certain best practices in a low risk environment may be sufficient to mitigate the risk present and enable the importer to qualify for Tier Three standing. However, in a high-risk environment, the adoption of the same practices may be viewed as a necessary, minimum security measure, and therefore not elevate the overall security environment to the point at which the importer would be considered for Tier Three. A determination of Tier Three eligibility is thus based on the totality of the security measures employed, not on any specific practice(s), and whether or not the overall security environment effectively addresses the risk adherent to that specific international supply chain.

C-TPAT Supply Chain Security Specialists are committed to working alongside members to help design the security measures necessary to address the risk, exceed minimum security standards, and thus enable the importer to achieve Tier Three standing and receive the greatest benefits afforded by CBP.

Tiered Benefits Structure

To ensure the success of C-TPAT, the security criteria or standards which members must meet or exceed must remain robust, dynamic, and within a flexible security framework, with the overall objective of elevating the security measures employed throughout the international supply chain. As C-TPAT members enhance their security measures to meet these clearly defined security criteria, CBP must also provide enhanced benefits. In May 2005, CBP moved to a three-tiered benefits structure, where C-TPAT importers who do more, receive more.

Under **Tier One,** *certified* importers receive meaningful risk score reductions, resulting in fewer cargo examinations for security concerns, a lower level of random Compliance Measurement examinations than those afforded to non-C-TPAT importers, and the negation of most trade cargo examine selectivity. These three conditions afford Tier One importers with a low level of examinations. Additionally, Tier One importers are also eligible for expedited cargo processing at the border (FAST lanes at the land borders), receive 'front of line' inspection privileges at ports of entry should an examination be required, are entitled to certain penalty mitigation for Trade Act of 2002 violations, become eligible for the Importer Self Assessment program, and may attend C-TPAT training seminars. CBP believes that the level of benefits afforded Tier One importers is commensurate to the level of commitment demonstrated by the C-TPAT member.

With the additional commitment demonstrated as a result of having successfully undergone a *validation,* the validated importer then becomes eligible for Tier Two or Tier Three status. An importer whose validation reveals that *minimum security criteria have been met* will receive Tier Two benefits. **Tier Two** benefits include all the same benefits associated with Tier One, but Tier Two importers are provided with twice the level of risk score reductions received by Tier One importers, resulting in significantly fewer examinations for security reasons than those received by Tier One importers.

Finally, for those importers whose security measures *exceed the minimum security criteria* and have adopted "security best practices" as evidenced by the successful completion of a validation, **Tier Three** status is granted. Under Tier Three, all benefits associated with Tier One and Tier Two are granted, and the most significant risk score reductions available are provided by CBP, resulting in very infrequent examinations for security reasons. Tier Three status is also the precursor for CBP's "Green Lane" which will afford members with zero inspections upon arrival except for an occasional random examination, contingent on meeting other "Green Lane" requirements, such as shipment through a Container Security Initiative (CSI) port, and the use of a container security device. CBP intends to roll out the "Green Lane" in 2006 once effective container security technology becomes available.

Tier Three Status

To help importers achieve the highest level of benefits provided, Tier Three benefits and the precursor to the "Green Lane," CBP has committed to outline "Security Best Practices" and work with members to adopt, modify, and implement those security best practices which will help take the member's security practices to the next level.

This inaugural edition of the *C-TPAT Best Practices Catalog* is intended to categorize specific security measures which C-TPAT Supply Chain Security Specialists have identified as 'best practices' resulting from the more than 1,400 validations conducted to date. This catalog will be a living document, updated periodically as additional validations are conducted and new security best practices are noted. The outlined "best practices" pertain to security procedures used throughout an international supply chain, such as conveyance monitoring and tracking, cargo tracing, preventing collusion, employee awareness, physical security and surveillance, and other areas crucial to supply chain security.

Corporate Governance Structure Supporting Supply Chain Security

As C-TPAT Supply Chain Security Specialists conduct security validations, one common, essential practice has emerged which is so significant to the overall supply chain security environment, that Tier Three status can only be obtained by the presence of this practice. That practice is a corporate governance structure through which supply chain security is embraced at the highest levels of the company—the CEO, the COO, the President, etc. The security of a company's supply chain should be a required topic of discussion in corporate boardrooms. Security of supply chains is often as important to the financial survival of a company as the accuracy of a company's financial statements. Supply chain security practices must be periodically reviewed for adequacy by CEOs and corporate boards, and noted deficiencies must be addressed timely.

Additionally, a unified corporate governance structure which embraces the importance of supply chain security has proven to be more effective in leveraging their corporate strength to require supply chain security practices and enhancements through their entire international supply chain, from all business partners. These security measures must be pushed back from the point of stuffing of the container or air cargo shipment, through the ultimate arrival of the cargo into a U.S. port of entry. The active engagement by top corporate officials in a company's supply chain security efforts cannot be understated, and as a result, the involvement by senior corporate leaders is a requisite for Tier Three status.

Management Support

Senior management support determines whether or not the appropriate resources (human, financial, and technological) will be dedicated toward improving supply chain security, and ensuring that security is a priority for the company as a whole. This support is demonstrated by senior management's involvement in and understanding of the company's supply chain security program.

Domestic

"Continuous Improvement" Philosophy: Company management integrated supply chain security into its business processes, practices, policies, procedures, and employee job descriptions. The Company considers security part of its "continuous improvement" business philosophy.

Proactively Engaged: Senior management from key departments (Information Technology, Purchasing, Contracting, Finance, Sales/Marketing, Shipping/Receiving, Transportation, Customs Compliance, Human Resources, and Facilities Maintenance) are fully engaged in overseeing and in some cases are actively involved in supply chain security initiatives. This support is demonstrated by their allocation of resources to security related programs and their participation in monthly security assessment meetings. Senior Management is proactively engaged in seeking ways to improve security measures for the company and its business partners.

Weekly Briefings: A President of a Highway Carrier provides breakfast to his dispatchers and drivers on Saturday. During that time, he conducts a meeting, provides training, and discusses transportation security concerns. The President documents topics discussed and employees who attended. Follow-up is conducted to ensure that absent employees remain informed.

Supply Chain Security Committee: A Supply Chain Security Committee was established by senior company executives to evaluate the Company's overall supply chain security and make recommendations for improvement. The Supply Chain Security Committee is comprised of senior managers, operational supervisors, line employees, and key management from foreign locations who are responsible for international supply chain security.

Top Management Knows Business Partners: Company's senior executive management maintains a high level of familiarity with its overseas agents, their practices, and affiliations by using formal and alternative methods to collect information. In addition, the company president has conducted extensive international travel to meet with buying agents to discuss factory and transportation provider security requirements.

Full Integration of Supply Chain Security Policies: Company executive management is committed to ensuring that supply chain security procedures are adopted by all of their subsidiaries, suppliers, and service providers worldwide. All company subsidiaries must develop and implement a sound security plan that addresses terrorist risks in the international supply chain and crisis management. Executive management reviews these plans to ensure their completeness and implementation.

Worldwide

Establishing Security Directors and Country Managers: An International Corporation has established Regional Supply Chain Security Directors and Country Managers worldwide to ensure that supply chain security procedures are implemented and consistently followed by factories and service providers. These Security Directors and Country Managers also are responsible for continual supply chain security risk analysis and contingency planning for the corporation.

Security Councils: Company established a Security Council to formulate global security guidelines, determine methods to evaluate security weaknesses, formulate action plans, and determine methods to control security procedures worldwide. Senior management at all locations is responsible for documenting actions they have taken to support and improve supply chain security practices.

Mission Statement: International Company has incorporated supply chain security into its mission statement.

Advanced Data/Entry Level Data Submission and ACE

Advanced data helps businesses and government detect anomalies and discrepancies prior to the cargo's arrival. In addition, advanced data increases the timeliness of critical information, enhances logistics planning, and helps to ensure an efficient, seamless, and secure supply chain.

Business to U.S. Customs and Border Protection

Advanced Trade Data Initiative / Entry Level Data Submission: To fully realize the reduced cargo inspection benefits afforded to C-TPAT importers, the Company participates in the Advanced Trade Data Initiative (ATDI) and/or transmits entry-level import data to CBP prior to loading the cargo onto the conveyance for shipment to the United States. Advanced trade data allows CBP to more effectively target high-risk shipments, while affording certified C-TPAT importers with reduced cargo inspections.

Automated Commercial Environment (ACE): Company has enrolled in U.S. Customs and Border Protection's Automated Commercial Environment (ACE) program to facilitate the transmission of entry information and automate all aspects of customs information exchange. The company actively uses the ACE Portal to monitor import transactions for anomalies.

Business to Business

Electronic Data Interchange (EDI): Broker and Company receive entry information electronically from the shipper prior to the cargo's arrival so that anomalies can be detected, discrepancies can be immediately investigated and resolved, and accurate information is declared to CBP.

Secure Electronic Data Transmissions: Company's shipments are traceable through secure electronic data transmissions. Information is updated at various points along the supply chain. All authorized parties have the necessary viewing privileges to plan appropriately for arriving/departing shipments, as well as the ability to immediately identify anomalies.

Advanced Shipping Notices (ASNs): Barcode pack and scan system allows vendors to transmit Advanced Shipping Notices (ASNs) and packing lists electronically to domestic distribution center. This system improves packing accuracy and reduces quantity discrepancies (overages/shortages).

Risk Analysis

Given the complexity of the international supply chain, a risk analysis is necessary to focus resources and prioritize action items. The more complex the supply chain, the more extensive the risk analysis becomes and consideration should be given to using risk models and developing organizational expertise. Risk analysis helps companies identify and address the most immediate threat(s) to their supply chain. As the political climate, business relationships, trade lanes, and modes of transportation change within a company's supply chain, a risk analysis is needed. Risk analysis requires constant communication with business partners and knowledge about their security measures.

Identifying Risks and Creating Remedies: Company conducted a comprehensive risk analysis of its international supply chain by researching terrorist/criminal activity in supplier countries. Company sent security surveys to all foreign suppliers and service providers. The surveys were used to develop detailed flow charts of the various supply chains and analyze the security measures used to secure shipments at each stage of cargo handling. The company's final step involved developing an action plan to address the gaps, vulnerabilities, and weaknesses that were identified and conduct follow-up with business partners. In addition, a risk analysis is performed for all new business partners.

Tapping Into Existing Resources: Air Carrier obtains information from CBP and/or the U.S. Department of State web sites on a regular basis to determine what cargo is of moderate or high risk for smuggling, sabotage, or terrorist attack. Air Carrier has established procedures to handle high-risk cargo, which include thoroughly reviewing customers' security procedures and rejecting cargo from "unknown" shippers in high-risk locations.

Keeping Key Personnel Informed: The Company's risk analysis and threat assessment are posted on the company's intranet, which provides guidance to buyers, logistics managers, and security personnel in determining necessary levels of security to protect corporate assets and prevent shipments from being compromised. In addition, senior management conducts follow-up with key personnel to ensure they are kept up-to-date on potential threats.

Self-Assessment

Self-Assessments enable companies to evaluate the effectiveness of the security measures used within their international supply chain. In addition, self-assessments help to identify the need for additional resources, as well as correct gaps, vulnerabilities, and weaknesses.

Domestic Facilities

Conducts Periodic Assessments: Self-assessments include periodic review and audit of security procedures, equipment, training, and other asset protection measures that directly affect the integrity of the Company's supply chain security.

Engaging Employees: Company selects employees in a random lottery to assist with weekly audits of inbound containers. This procedure affords all employees, even those not in cargo-handling jobs, the opportunity to be involved in the company's supply chain security program through first-hand experience. These audits include seal and inventory verifications.

Weaving Security Into Business Practices: Company has incorporated supply chain security into its internal management audits. This practice fully integrates security into business practices.

Verifying Container Inspections and Conveyance Tracking: Highway Carrier President periodically conducts audits of container/trailer inspections performed by drivers to ensure they are consistently conducting inspections before leaving the truck yard and the customer's facility. President also periodically follows drivers on their routes and listens in on dispatcher, receptionist, and driver communications to ensure that there is no collusion.

Verifying/Rotating Security Guard Duties: The Company Security Manager verifies that guards are performing their duties, especially during the night shift. A periodic review of the guards' activity logs and incident reports is conducted, and incomplete/inconsistent information is addressed. Guards are also rotated to avoid complacency and internal conspiracies.

Verifying Physical Security: Inspections of the facility's physical security are conducted and documented as part of the guard's routine responsibilities. Each day, the guard is required to verify that alarms, generators, video surveillance camera systems, and access control devices are working, and that fence lines are maintained.

Foreign Facilities

Holding Business Partners Accountable: After the Company's C-TPAT validation, follow-up meetings and site visits were conducted with foreign suppliers and service providers to evaluate their progress against the C-TPAT Security Criteria. As part of its plans to regularly inspect supply chain partners for security compliance, the Company will conduct several unannounced on-site security inspections of its suppliers and service providers. In addition, the Company amended supplier and service provider contracts to incorporate minimum-security requirements and initiated risk-based audits.

Incorporating Security Into Factory Audits: To complement the Company's Factory Audit Program, the Company conducts random security audits of high-risk foreign manufacturers. These random audits serve as another check and balance to ensure foreign manufacturers comply with the Company's security policies. These audits also allow the Company to observe the security measures utilized in their supply chain first hand and discuss the contractual supply chain security requirements with their foreign manufacturers.

Utilizing Overseas Resources: Company routinely monitors factory, supplier, and service provider security by using buying agents stationed overseas who have been trained by a security firm on how to conduct security site verifications.

Utilizing External Resources: A certified C-TPAT Partner hired a security firm to physically verify that all primary overseas factories adhere to C-TPAT Security Criteria, as agreed. During factory site visits, the Company's employees participate in the verification to ensure direct company involvement.

Security Planning and Program Management

Effective supply chain security involves a comprehensive and holistic approach to ensure the right people, processes, and technology are in the right place at the right time to prevent a security incident. A comprehensive understanding of the operations, interrelationships and interdependencies within the supply chain is critical to establishing a supply chain security program. Supply chain security must be integrated into a company's business processes to be effective.

Holistic Approach to Security: Company uses a holistic approach by first determining the business interrelationships among departments within the organization and with foreign suppliers/service providers. With the collaboration of key domestic department managers and employees (Purchasing, Shipping/Receiving, Human Resource Management, Logistics, Information Technology, Facility Maintenance, and Planning/Operations) and foreign business partners, the Company formulated an international supply chain security program and established a system of checks and balances to ensure that security measures are working. The Company incorporated security risk assessments into its supply chain management plan.

Establishing Internal Networks: Sea Carrier has established an internal network of regional security representatives who are responsible for the integration of security procedures into new projects, in addition to their traditional role of responding to security incidents.

Global Security Management: International Consolidator restructured security force to address global supply chain security issues. Responsibility for all security rests with the Global Security Manager who oversees District Security Managers, Field Security Managers, and Investigators. The clear line of authority and organizational structure has increased the visibility and importance of security throughout the organization.

A Plan For Continuous Improvement: To ensure continued compliance and improvement is part of the Company's ongoing and future commitment to supply chain security, the Company created a program consisting of awareness, compliance, and training. First, the Company continuously promotes an awareness of supply chain security measures to their managers, employees and service providers. Second, internal policies have been updated and a checks and balance system has been established. In addition, supply chain security policies, job descriptions, and the vendor guide have been updated, and security measures have been added to service provider contracts. Third, the Company developed training to keep employees and service providers up-to-date on supply chain security issues.

Interpersonal Relationships and Worldwide Networks: To effectively achieve supply chain security worldwide, the Company has established strong interpersonal relationships and networks to understand the culture of their business partners. This understanding enables the Company to work effectively with their business partners to implement supply chain security recommendations.

Business Partner Requirements

Where a company out sources or contracts elements of their supply chain, such as a foreign facility, conveyance, domestic warehouse, or other service, it is imperative that the company work with its business partners to ensure that security measures are in place and adhered to throughout its supply chain. The following Best Practices illustrate the leverage, influence, and follow-through of C-TPAT Partners to achieve effective supply chain security worldwide.

Manufacturer/Supplier/Vendor Requirements

Requiring Security Adherence: A C-TPAT certified company is promoting supply chain security by conditioning its business relationships on C-TPAT Security Criteria. The company requires that all business partners accept and implement the C-TPAT Security Criteria, if they wish to continue to do business. For example, the Company's new purchase orders include the language "Supplier accepts responsibility for factory and container security until such time as the container/merchandise is delivered to the ocean terminal, authorized yard, or consolidation point. Supplier will immediately report container seal changes and reason for changes to the U.S. Distribution Center Manager."

Holding Buying Agent Accountable: Company established a Vendor Compliance Manual that outlines the security requirements for overseas factories. All overseas buying agents must use the Vendor Compliance Manual when selecting a factory on behalf of the Company. Moreover, the manual lists freight forwarders approved by the Company that must be used to ensure continuity of supply chain security standards.

Contractual Obligations: Company has incorporated into its contracts with foreign suppliers and service providers a requirement that security gaps, vulnerabilities, and weaknesses must be addressed immediately. They also are subject to random security audits to verify compliance.

Requiring Business Updates: Company requires semi-annual "business updates" from all of their international service providers and suppliers that include identification of changes in business operations (e.g., security measures, management changes, employee turnover, policy/procedural changes with respect to packaging/cargo handling and storage, political climate, financial status, and contract changes with service providers). This information is used to analyze risk, determine contractual compliance, ensure continuity of established supply chain security measures, and identify the need for changes/modifications to security plans.

Factory Certification Requirements: Company's factory certification program has an established rating scale to assess the level of adherence to the Company's security policies and procedures. Only those manufacturers who receive a passing score are permitted to do business with the Company. This system encourages factories and suppliers to comply with the Company's security standards and improve deficient areas.

Supplier Code of Conduct: Company developed and implemented a Supplier Code of Conduct as part of its Supplier Business Requirements. The Supplier Code of Conduct requires suppliers

to understand the key integrity performance criteria required of them, including supply chain security.

Collaborating to Select Suppliers and Service Providers: Company's export/import, transportation, purchasing, and finance departments take part in supplier and service provider selection/renewal. These four key departments work together to ensure that operational and security problems are addressed and corrected by suppliers and service providers before contract renewal. This collaboration creates system of checks and balances for the service provider and supplier selection process.

Managing Non-Compliant Essential Business Partner: If a supplier is unable to meet C-TPAT security criteria or is uncooperative with the Company, but is deemed a "critical" supplier by the Company, measures are taken to address the supplier's security vulnerabilities by closely scrutinizing the shipments from that supplier. The Company will notify its assigned CBP Supply Chain Security Specialist of concerns with the supplier and develop a plan of action to address these concerns.

Service Provider Requirements

Exclusive Representative: An account representative at the foreign freight forwarders office is specifically assigned to the Company's account to ensure continuity and detect unusual or suspicious activities.

Prohibiting Subcontracting: Company included a clause in highway carrier contracts whereby shipments cannot be subcontracted to other carriers without breaching the contract. The contract states that, "Highway carrier will be subjected to legal and financial consequences if subcontracting occurs." This contract clause helps to ensure cargo control and consistent security measures.

Requiring Background Clearances: Company requires that all service providers (janitorial, transportation, personnel, etc.) conduct comprehensive criminal background investigations on contract employees. In addition, the service provider must submit bio-data with pictures and copies of the background investigations conducted on employees referred to work at the Company.

Contractual Obligations: Company has incorporated security into its contracts with service providers. Such requirements include, but are not limited to, conducting an inspection of all empty containers/trailers prior to loading and documenting inspections; establishing seal control, issuance, affixing, and verification policies with appropriate checks and balances; tracking driver movements throughout transport; establishing access controls to the Company's cargo; and screening the employees who handle their cargo. These requirements are also subject to on site verifications.

Establishing Procedures for Selection: Extensive written standards specify requirements for the service provider selection process, which include security. Company verifies the veracity of the service provider's security measures, financial solvency, and business references by conducting follow-up both in person and over the phone. The veracity of the service provider's claims will determine whether or not the Company will continue to do business with them.

Customer Screening

Preventing Misuse of Products by Customers: Chemical Company requires that sales representatives screen customers who use its products to ensure purchases are for legitimate use. In addition to financial information, sales representatives must complete an "Indicators of Suspicious Activities" form for each new customer. The sales manager must review the form before the customer is approved.

Requiring Original Power of Attorney: Broker has a procedure for pre-screening customers prior to engaging in business. The Broker verifies business references, runs credit and business reports. The Broker will not accept cash payments or requests made over a cell phone. This practice reduces the chance of the brokerage firm being used by an unknown party for unlawful purposes. In addition, the Broker requires from clients and freight forwarders an original Power of Attorney that must be notarized before initiating transactions.

Keeping Current with Customer Information: The Broker subscribes to a business information service to monitor his clients' business status and identify unusual trends and financial problems.

Managing the Unknown Customer: Air Consolidator has a database that helps to distinguish known shippers from unknown shippers. Measures are in place to closely examine and segregate unknown shipper transactions. Under the supervision of an operations manager, the cargo is examined and a form is completed which documents the type of examination performed along with the results. All unknown shippers must have a verified business referral.

Requiring Customer Registration: Consolidator requires customers to register as "Known Consignors," whereby they must sign a declaration that has legal implications. The declaration also states that specific security measures have been taken before delivering cargo.

Using External Resources to Screen Customers: Before transporting cargo, Highway Carrier President requires all new customers to complete a credit application and verifies commercial and bank references. Certified check or cash transactions are prohibited. In addition, the customer's reputation is checked through the local trucking association and business contacts.

Requiring Business Referral: Freight forwarder requires that the U.S. Importer of Record introduce all new shippers and will not do business with unknown entities.

Meeting with Customers In-Person: Highway Carrier's management makes it a priority to get to know customers, customers' employees, and their security measures. Customers are required to complete a security questionnaire and a business profile that includes a request for financial information and business references. Highway Carrier's management then makes a personal visit to the premises of each new customer (and periodically to existing customers) to verify security measures, particularly for product packaging, staging, container/trailer inspections, and seal control. In addition, for each new customer, reference checks are conducted and information is verified to ensure the customer is legitimate. If the customer's security is found to be inadequate, the Highway Carrier works with the customer to increase security or may decide to discontinue doing business with those unwilling to participate in supply chain security measures.

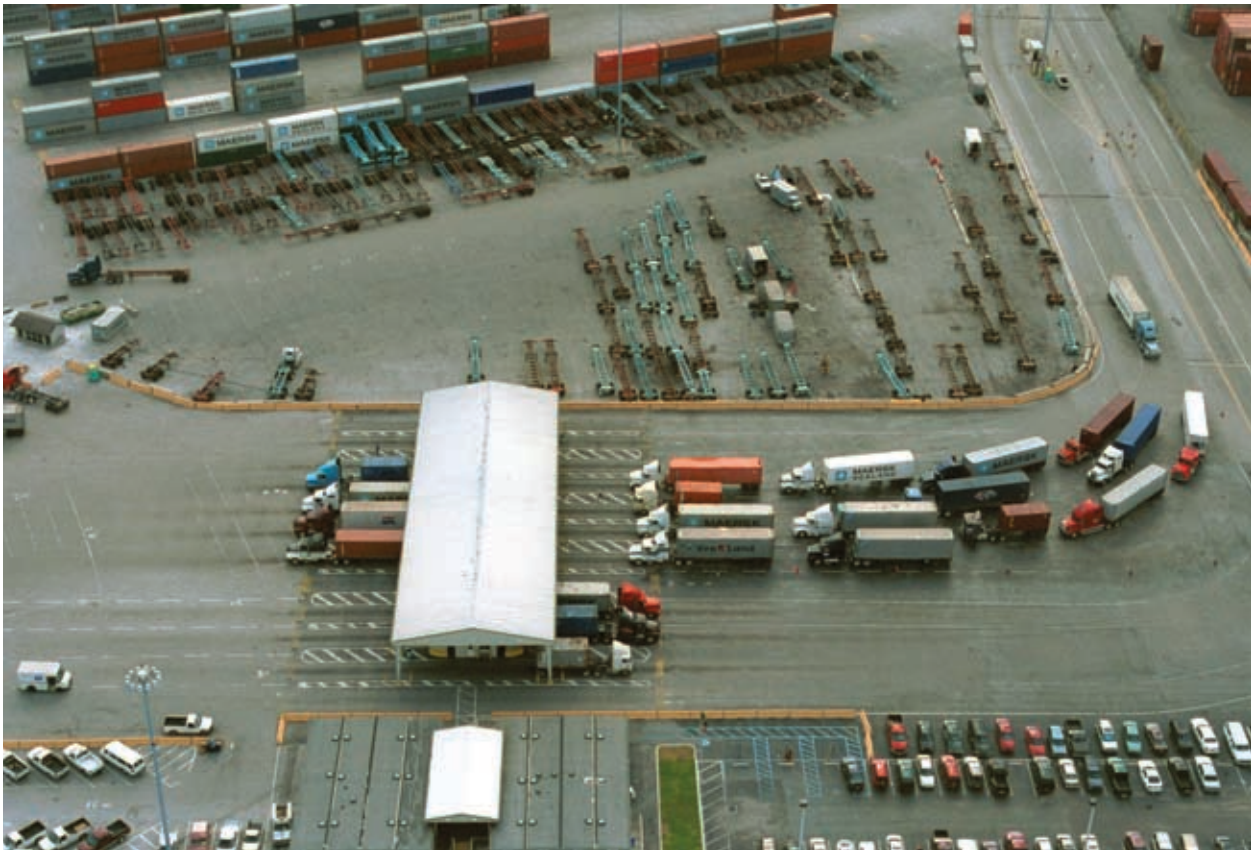
Requiring Customers to Inspect Containers: Highway Carrier requires customers to inspect empty trailers prior to loading if the Highway Carrier's drivers are not present to inspect and witness the loading. Highway Carrier also informs the customer that it will use a contracted security company to perform an inspection of the container/trailer prior to crossing the border.

Refusing Pick-Ups from Unknown Locations: Highway Carrier will not pick up cargo at an unknown location and works with customers to establish routine pickup locations. This procedure helps the Highway Carrier to immediately detect deviations, anomalies, and suspicious activities.

Sending Representatives to Meet with New Foreign Customers: Freight Forwarder has integrated into its security program the procedure of sending a representative to meet with and verify the physical location of all new foreign customers. Freight Forwarder's representatives are responsible for inquiring about customer's security, composing information sheets, reviewing references and conducting financial checks.

Customer Outreach

Reaching Out to Customers: Highway Carrier sent a letter to all customers expressing its commitment to develop and implement a reliable plan to enhance supply chain security. The letter strongly encourages the customers to enroll in the C-TPAT program and specifies the minimum security requirements that customers are expected to meet.



Container/Trailer Security

Container security is a requirement for many C-TPAT Partners whose companies and/or foreign shippers/suppliers stuff containers at the point of origin. Container security measures involve container inspection, storage, and tracking, as well as seal control, issuance, and verification throughout the supply chain. A 7-point inspection specifically refers to the following areas of container's/trailer's structure: front wall, left side, right side, floor, ceiling/roof, inside/outside doors, outside/undercarriage. As technology becomes available, C-TPAT partners are encouraged to explore the use of technology such as the "Smart Box" to secure their containers. The following best practices have been identified for container security.

Container/Trailer/Unit Load Device (ULD) Inspections

Domestic Highway Carrier Drayage

Inspecting at Domestic Container Yard: Contracts with local drayage highway carriers include the requirement that drivers must thoroughly inspect the exterior of the container, verify the container and seal numbers, and ensure that the seal is in tact prior to transporting the container to the distribution center. Before accepting the loaded container, the driver must report anomalies to the distribution center's receiving manager who in turn will notify CBP of the anomaly.

Foreign Highway Carrier

Securing Empty Containers: Once a customer pick-up order is placed, the driver conducts and documents a 7-point inspection of the container/trailer using a checklist. The driver must sign the inspection checklist and the Highway Carrier's security guard verifies the inspection and signs the checklist. The guard then places a numbered plastic seal on the trailer, documents the seal number on the delivery trailer/container order, and calls the factory to notify the shipping department of the seal number. The driver verifies the plastic seal number that the guard has placed on the container/trailer by initialing next to it. Upon arrival at the factory, the driver presents the pick-up order to the factory security guard. The factory security guard verifies the seal number upon arrival and signs the inspection sheet. The factory conducts another 7-point inspection prior to stuffing.

Securing Container/Trailer After Customs Examination: The driver must notify the factory and his dispatcher if a customs examination of the cargo is required. After the examination, the factory's broker (who is stationed at the border) places a new seal on the container that is verified by the driver. The broker calls in the new seal number to the factory, highway carrier's dispatcher, and distribution center in the United States. The new seal number is annotated on the bill of lading and is initialed by the broker and the driver. The driver calls his dispatcher to confirm the new seal number.

Detecting False Walls/Compartments: A Highway Carrier uses several low cost, commercially available laser measuring devices to detect false walls, compartments, and hidden contraband. One

device is used to measure the dimensions of empty containers and compare the findings against standard measurements. A mirror is used to inspect the undercarriage of the container.

Air Carriers

Screening and Inspecting ULDs on Passenger Flights: An Air Carrier has established special security measures for passenger flights carrying cargo. First, the carrier will not accept containers/ULDs from unknown customers. Second, known customers are informed that their cargo is subject to random inspections. Third, the carrier conducts and documents a 7-point inspection on all empty ULDs/Containers and places a seal on the container.

Establishing Written Procedures for ULD Inspections: An Air Carrier has developed a comprehensive written container/ULD inspection procedure that incorporates the use of a checklist to ensure that the container is completely inspected. Individuals responsible for ULD/container inspections must certify their inspection by printing their name, as well as signing and dating the form. Management audits these checklists periodically.

Consolidators

Conducting X-Ray Examinations: In addition to the airport screening process, the foreign Airfreight Consolidator x-rays all incoming cargo.

Factory/Supplier/Vendor

Inspecting and Weighing Empty Containers: The Factory conducts a 7-point inspection and weighs every empty container/trailer prior to stuffing. The security guard, shipping manager, and driver (if present for stuffing) verify these inspections by signing off on the inspection checklist. In rare instances where the empty container is not loaded immediately, a padlock and plastic seal are placed on the door. Later the seal is verified before opening the empty trailer/container for stuffing to ensure its integrity.

Photographing Container and Seal: After the container is loaded at the factory, a digital picture is taken of the back of the container before the doors are closed and sealed. After the container is sealed, digital pictures are taken of the seal and all sides of the container. The pictures are transmitted to the port terminal operator and to the distribution center in the United States.

Terminal Yards/Operators

A Team Approach to Container Inspections: Terminal Operator organizes a "checker team" to inspect, weigh and log every container entering and exiting the terminal. An exterior inspection is performed on full containers and a 7-point inspection is conducted on empty containers to ensure their integrity. The checkers input information regarding the container into the terminal's database and crosscheck information provided by the shipper to detect anomalies.

Container Seals

Domestic

Utilizing "Smart Box" Technology Sea Containers: As technology becomes available and more reliable, CBP recommends the use of "Smart Box" technology to increase a company's ability to determine whether or not the container has been compromised while moving through the supply chain.

Verifying and Disposing of Seals: Seal numbers are verified at the distribution center by writing the number of the actual seal next to the seal number listed on the shipping documentation. This procedure provides a written record that the actual seal was checked and verified against the seal number listed on the shipping documentation. The shipping supervisor must be present to verify the seal before it is broken. He/she gathers and secures broken seals to prevent their misuse.

Sea Carrier

Logos on Seals: Sea Carrier requires the use of individually numbered high security bolt seals that bear the its logo. The Sea Carrier also requires that this seal be placed all empty containers laden on its vessels. Each dispatched container is assigned a specific seal that facilitates tracking the origin of the container.

Modifying Containers: Sea Carrier requires seal checks at every interchange throughout the container's transport. In addition, the Sea Carrier has modified the structure of its ocean containers. Rather than use the hasps on the door to affix the seal, carrier uses a locking point mounted on the lower sill of the container structure. This prevents the drilling of the round-head bolt used to secure the hasp, a method used to open container doors while keeping the seal "intact."

Highway Carrier

Utilizing Plastic Seals to Secure Empty Containers: Plastic seals are placed on empty inspected containers that are stored in the truck yard. Seals are verified when the guard conducts his rounds. Unused plastic seals are secured in a locked cabinet, logged, and reconciled.

Highway Carrier

Tracking Seals Given to Drivers: During long haul transport, an extra seal is maintained inside the trailer in a tamper evident envelope in case the trailer needs to be opened for government examinations while in route. If the seal is used, the original seal must be placed inside the trailer, the new seal number is called in to the dispatcher, and all concerned parties are notified of the seal change. If the seal is not used, the envelope must be returned to the dispatcher.

Seal Control and Verification: Highway Carrier issues high security bolt seals and cable seals to their customers before drivers pick-up cargo. The seals are secured, tracked, and verified. At cargo pick-up, the Company guard, shipping manager, and driver are present when the seal is placed on the container. All parties present for the affixing of the seal must initial the bill of lading to

document their verification. The shipping manager then calls in the seal number to the trucking company dispatcher and the customer in the United States. The seal number must be within the range of seal numbers issued to the customer by the highway carrier.

Factory

Establishing Seal Control Policy: Factory has comprehensive written policies and procedures regarding container seals that include: accountability and responsibility for how seals are controlled, issued, secured, affixed, and verified throughout the supply chain. The policy also specifies how the seal inventory is maintained and reconciled.

Holistic Approach to Seal Control: Seal numbers are electronically transmitted by the Factory to the Highway Carrier and the importer of record before the truck's arrival at the factory. The truck driver and security guard witness the placement of the seal by the shipping manager and check the integrity of the seal. The seal number is documented on the bill of lading. The guard and driver must initial next to the seal number on the bill of lading to attest to their verification of the seal. Before leaving the factory, the driver calls in the seal number to his dispatcher who verifies the seal number against the electronically transmitted number. The guard stationed at the gate verifies the trailer number and seal number before the driver leaves the factory. The guard also initials the bill of lading and records the seal number on the truck exit log.

Multi-National Corporation

Global Seal Control: Company established a uniform policy for all its subsidiaries and service providers regarding seal issuance, control, and verification to ensure product integrity and security throughout the supply chain. Tamper evident seals are affixed and repeatedly verified throughout all changes in custody. Seal changes are communicated to all parties (shipper, importer, highway carrier, terminal, freight forwarder, etc.). The seal number is transmitted to each handling point via secure electronic data transmissions and is verified before acceptance at each handling point.

Consolidator

Segregating and Sealing Less Than Truck Loads (LTLs): Consolidator's trailers have been modified with several partitions to segregate each consignee's cargo to enhance the security of LTL cargo while in route from the factory/shipper to the Consolidator's warehouse. The seal number is recorded on the pick-up order and the factory calls in the seal number to the consolidator at the time of pick-up. The consolidator verifies the seal numbers upon the truck's arrival.

Tracking

Terminal Operator Container Yard

Addressing Unusual Occurrences: Terminal Operator created a system to detect "unusual" requests and time lags for empty containers dispatched and returned to the yard. When customers order containers, the Terminal Operator initiates a screening process. This process involves obtaining information regarding the amount of time the container is needed, type of cargo, credit

information, and positive identification of the customer. In addition, the automated container tracking system generates an alert for containers that are "out of time range" and the container is flagged for an inspection upon its return to the container yard.

Highway Carrier

Identifying and Reporting Anomalies: Highway Carrier developed a spreadsheet to track the time that trailers remain at customers' premises to identify unusual delays. For containers that are out of the normal time range, the Highway Carrier contacts CBP to report the anomaly and request a courtesy examination of the trailer.

Controlling Use of Equipment: Highway Carrier will not permit customers to reroute their trailers to another facility. In addition, Highway Carrier maintains strict control of their equipments' use and location.

Storage/Inventory

Container Yards

Managing Container Inventory: Container yard has established a bar code container inventory management system to track and monitor all empty containers staged in their yard. The system ensures that empty containers do not remain in the yard for more than an established period of time and helps prevent exposure to tampering.

Highway Carrier Truck Yard

Storing Containers: Loaded and empty containers are stored door to door and are sealed to prevent unauthorized access.

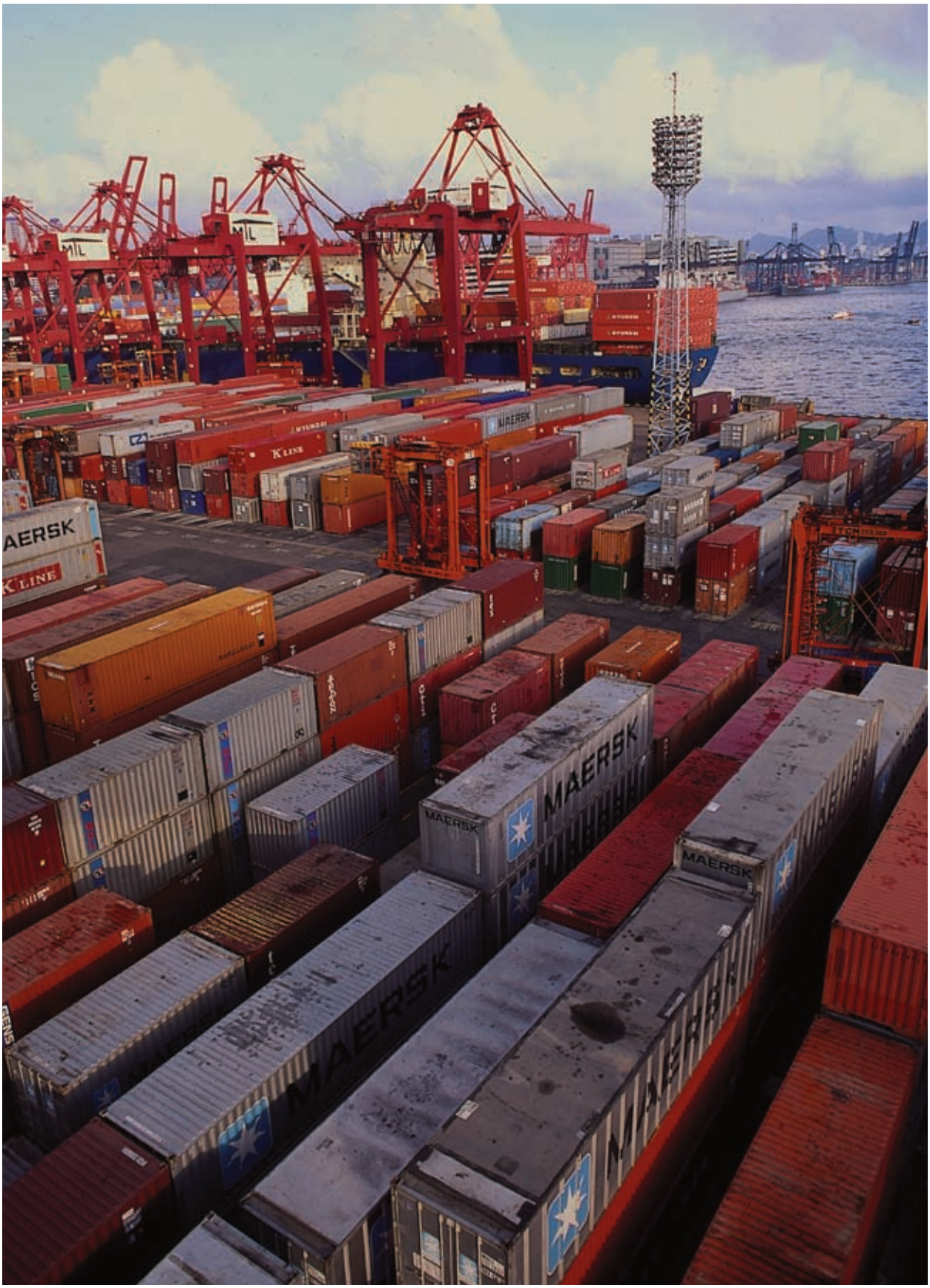
Assigning Parking Spaces: Highway Carrier has assigned parking spaces for trailers and containers to facilitate equipment inventory. In addition, a plastic seal that is controlled and tracked is placed on all empty trailers. The security guard is given a map of the parking assignments along with seal numbers to conduct inventory and verify the integrity of the seals throughout his shift.

Consolidator

Protecting Unsecured Containers: Consolidator invented a steel plate that protects the contents of open containers while cargo is not being loaded/unloaded. A large cement block is placed in front of the steel plate, making it impossible to be moved without mechanical assistance.

Air Carrier

Controlling Access to ULDs: Air carrier stores empty and full ULDs in a secure location where access is controlled and documented. The Air Carrier uses a ULD inventory system to immediately identify the location of its equipment.


MIL
MIL
MAERSK
K LINE
AERSK
K LINE
MAERSK
MAERSK
MAERSK
MAERSK

Conveyance Security

Conveyance security is critical to ensure that the mode of transportation is not used to facilitate a terrorist or other illegal act. Inspecting, securing, and tracking conveyances are essential measures in preventing the conveyance, container and cargo from being compromised en route. C-TPAT partners are encouraged to use technology to accurately track conveyance movements and detect deviations.

Conveyance Inspections

Air Carrier

Using Inspection Checklist: Air Carrier developed a comprehensive conveyance inspection checklist that specifies each area of the aircraft that must be inspected. Areas include, but are not limited to, baggage hold areas, overheads, lavatories, galleys and food carts, cockpit and electronics areas, wheel wells, and landing gear. In addition, the inspection must be documented and the individual conducting the inspection must print and sign his name and date the form. Management routinely audits these inspection reports to ensure that they are performed.

Highway Carrier

Reinspecting Conveyance While in Route: Highway Carrier's security guards/drivers inspect conveyances entering and exiting the facility and use a detailed conveyance inspection checklist to identify modifications to the tractor. Re-inspections are required after intermediate stops. The checklist is maintained for an established period of time for each inspection. Management periodically reviews the inspection checklists and participates in inspections to ensure they are performed thoroughly, consistently and accurately.

Sea Carriers

Detecting Stowaways: Sea Carrier uses canine patrols and carbon dioxide detectors to detect stowaways on vessels at each port of call before sailing.

Conveyance Storage

Highway Carrier

Assigning Parking: Highway Carrier has assigned parking spaces for conveyances and trailers to facilitate the guard's inventory and ability to quickly identify missing equipment.

Collaborating to Establish a Secure Yard: A group of Highway Carriers established a secure yard to store full and empty trailers, containers, and conveyances.

Conveyance Monitoring

Highway Carrier

Installing Panic Buttons: Highway Carrier installed panic buttons in each tractor. In the event of an emergency or perceived threat, the driver can depress a button that will send an alarm signal to the dispatch office and to the Highway Carrier's top five managers' cell phones. The Highway Carrier identifies the location of the driver by using GPS tracking and dispatches company personnel. It also alerts local law enforcement and CBP at the border.

Establishing Check Points in Route: Highway Carrier has established several physical checkpoints along the 6–8 hour route. Highway Carrier uses these checkpoints to verify the integrity of the seal and the condition of the container. Management periodically verifies that drivers are stopping at established checkpoints and calling in, as required. If the driver fails to stop at a check-point or call-in, an escalation matrix is in place that includes procedures to contact the Highway Carrier's management up to and including contact with local authorities and CBP to conduct a full examination of the container upon its arrival at the port of entry.

Establishing Check Points at the Border: Prior to crossing the border, the Highway Carrier contracts with a private security company which uses dogs to detect contraband. In addition, the private security company takes digital photos of all sides of the trailer and a close-up of the seal. The digital photos are e-mailed to the Highway Carrier for verification before releasing the driver to cross the border.

Security Code Words: Highway Carrier assigns each driver a code word in order to alert the dispatcher of a threat so that police can be called. Code words are also used to identify locations along the route where the driver can be found.

Highway Carrier

Utilizing Security Escorts: In high-risk areas, Highway Carrier uses security guards to escort tractor-trailers to provide additional security for the drivers, cargo, and equipment. Throughout the container's transport, the security guard keeps the container in plain view and communicates with the truck driver via radio/cell phone communication.

Stationing Employee at the Border: Highway Carrier has an employee stationed at the border to monitor arrival times. If there is a significant unexplained time variance, the Highway Carrier's employee will contact CBP to "red flag" the shipment for a courtesy examination.

Utilizing Tracking Technology: Highway Carrier has GPS tracking and text messaging on all tractors. The tracking system enables text communication between dispatchers and drivers. Distress messages can be sent through satellite communication to dispatchers who

will, in turn, contact the local authorities. In addition, the GPS system is closely monitored to detect anomalies, unscheduled stops, and route variances.

Tracking Incoming/Outgoing Vehicles: Tractor movements into and out of the yard are recorded using a handheld electronic device that captures driver and tractor information.

Periodic Review of GPS Reports: Senior Management periodically reviews GPS reports of driver movements.

Maintaining Communication with Drivers: All of the Highway Carrier's drivers are issued radios and are required to call dispatch when they arrive at the client's facility, when they arrive at the border, when they clear foreign and U.S. customs, and when they drop the trailer at the customer's premises. Dispatch will input these times into a spreadsheet and verify that the times reported are accurate by matching the time reported with the time stamped on the paperwork by foreign and U.S. customs. The dispatcher contacts the customer to confirm the driver's arrival time.

Designating Routes: Drivers are given specific routes to follow and are only allowed to stop at designated areas. Average travel times, during peak and non-peak travel times, are known.

Utilizing Multiple Monitoring Methods: Highway Carrier uses multiple methods of tracking conveyances such methods include: timing driver movements in accordance with the standard time it should take from the point of pick-up to the border crossing; examining fuel consumption to detect route deviations; and establishing alternate routes in case of accidents or road construction. In addition, carrier provides drivers with two-way radio cell phones and requires drivers to call in their location upon arrival and departure from the factory, periodically in route to the border, upon arrival at the U.S. distribution center, returning to the border, and arrival at the next pick-up point.

Spot Checking by Management: Highway Carrier management conducts spot checks on drivers' routes and dispatcher call-in logs. If a driver fails to check in at any point, the dispatcher is required to follow-up with management and contact CBP to request a courtesy examination.

Monitoring For Collusion: Highway Carrier monitors communication between the driver, dispatcher, and receptionist to detect internal conspiracies. In addition, Highway Carrier rotates dispatcher assignments and administrative staff to prevent collusion.

Responding to Route Deviations: Highway Carrier uses GPS to track driver movements. When a driver deviates from his route and does not communicate with the base station, the Highway Carrier's dispatcher monitoring the movement will shut off the tractor's engine, lock the trailer so that it cannot be detached from the cab, call the police, and send a company guard to the tractor-trailer's location. Highway Carrier also uses air compression devices to automatically release air into the tires to prevent a flat when the driver is in route to a destination.

Traveling in Convoys: All trucks travel in convoys of four to six vehicles. Each driver has a two-way radio/cell phone and can contact every truck in the convoy.

Driver Check-In Alert System: To closely monitor drivers, Highway Carrier hired a programmer to develop an automated system that alerts the dispatcher when the driver has failed to check-in within a specified period of time.

Sea Carriers

Satellite Monitoring: Vessel Operator has a system that is monitored by a third party specializing in satellite tracking systems for vessels. Most noteworthy about this system is the internal code of communication between the vessel operator and the third party. If intruders compromise the vessel, the vessel operator has established a way to communicate the need for help to the third party without alerting the intruders.

Barge Transshipments

Remote Surveillance: Barge Carrier monitors the loading, transport, and unloading of containers from the barge by using CCTV cameras. The barge also is equipped with a GPS satellite system to monitor the barge's location.

Cargo Tracing in Route

Increased supply chain visibility has many benefits. Visibility allows a company to achieve increased supply chain security and control over inventory management, service providers, and cargo flow. Visibility permits the company to immediately identify and correct problems as the cargo moves through the supply chain.

Utilizing Scanning Cards: Details of the transported shipment are transmitted electronically to the Company through the use of a bar-coded plastic card. Carried by the driver, the card is scanned at each location along the supply chain and provides constant updates to the Company's inventory system. This control mechanism provides a real time snapshot on the status of each shipment.

Tracing Cargo with Driver Data Port: Company is able to monitor over-the-road cross border shipments through the use of technology that transmits data to the Company from the highway carrier's trucks. The truck is equipped with a data port and the driver is able to transmit messages concerning his location and delays. This system enhances the Company's ability to monitor its inbound shipments.

Logistics Tracking System: Company uses an automated system to track the status of shipments worldwide. The system allows the Company's representatives to manage orders and track shipments. The system is fully supported by the Company's information technology personnel. The Company also has used this system for security purposes to track unusual delays or anomalies that may point to illegal activity.

Physical Access Controls

Access controls prevent the unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. In addition, access controls regulate the movement of people and products to meet the operational needs of a facility.

Planning

Diagramming and Analyzing Access: Company diagramed and analyzed all of its facility's entrances and exits. They then identified all access control security features for the entrances and exits and proceeded to identify and correct gaps, vulnerabilities, and weaknesses.

Employees

Utilizing Biometric Technology: Company uses a biometric handprint identification system together with a 4-digit employee code to access work area and authenticate identities.

Color-Coding Uniforms: The factory uses color-coded uniforms for its employees to easily distinguish employees from truck drivers, contractors, vendors, and visitors. These uniforms also help identify employees outside of their work area.

Monitoring Access Patterns: Company periodically reviews proximity reader system to identify unusual patterns of employee access.

Terminating Facility Access: When an employee is terminated at the Factory, an information notice is issued to workers that the terminated employee is no longer permitted access to the Factory. A list of names and photos of the terminated employees are given to security to aid them in the access control of the facility.

Renewing Identification Cards: Company requires that employee identification cards must be renewed on an annual basis.

Temporarily Suspending Access: During extended absences, the employee's access privileges to the facility and information systems are temporarily suspended until his return.

Restricting Access: Proximity cards with photo identification are used by employees to gain access to different areas of the facility based on their job function. Employees' entry and exit times are restricted according to their work schedule. If an employee scans in and does not scan out of a particular area or vice-versa, the employee will lose his access privileges to the entire facility and an alert is generated. Attempts to access work areas outside normal hours are recorded and investigated. The employee must report to the Security Department to regain his access privileges. "Tailgating" is strictly prohibited, and employees are subject to disciplinary action for violation of this policy.

Requiring Employee Identification: Security guards verify that all employees wear their photo identification badges. Employees who do not have identification are detained until their manager can secure a temporary identification badge for them.

Visitors

Establishing Database for Visitors: After the receptionist verifies the visitor's identity and appointment time, the visitor is required to type his name, address, and contact information into a database. The receptionist compares the information entered against the visitor's identification. A photo of the visitor is taken and stored in the database along with the visitor's information. A temporary visitor's ID badge is printed and exchanged for the visitor's government issued identification (e.g., driver's license or passport). The visitor's ID expires at the end of the day. Management periodically runs reports to identify unusual visit patterns.

Establishing Multiple Visitor Check Points: Terminal Operator's visitors must stop at the Port Authority to obtain a pass. After presenting ID and a valid reason for being at the port, the visitor's picture is taken and a 1-day visitor's ID badge is issued specifying the area(s) he is permitted to visit. To be eligible for the pass, the visitor must meet an entity that is authorized to do business inside the port and be escorted at all times. Visitor badges are checked at various security points and badges must be returned at the end of the visit.

Requiring Pre-Clearance: Foreign Port requires that all visitors must be pre-cleared at least 3 days in advance of their visit. Pre-cleared visitors must show a government issued photo identification that is exchanged for a port visitor's badge. Visitors also must go through a metal detector and personal bags are x-rayed and searched.

Verifying Authenticity of Identification: Security personnel verify the authenticity of identification by using an I.D. Checking Guide that depicts license designs from all over the United States and the world. The Human Resources Department also uses this guide to verify the authenticity of state documents.

Deliveries/Cargo Pick-Up (Including Mail)

Terminals/Port Authorities

Exchanging Official Identification for Visitor's Badge: Terminal Operator requires drivers to enter the first access gate and exchange their driver's license for a visitor's badge. The Terminal Operator's guard records the driver's identification, truck number, seal number, and container number. The driver must then stop at the Sea Carrier's office to present his job order sheet and pay the entry fee. The driver then proceeds to the second access gate. The Terminal Operator will once again verify the container number and seal number and direct the driver to the yard location.

Scheduling Pick-Ups: To control access, the Terminal Operator established an appointment office to schedule driver pick-ups. The success of this system is dependent on the communication between the Terminal Operator and its business partners. Empty and full containers arrive at the

Terminal Operator's checkpoint where the Terminal's employee verifies the driver's appointment time. The driver is not permitted to enter unless the appointment is confirmed and the vessel is ready for loading.

Requiring PIN Number: Terminal Operator requires the use of a PIN number that is issued by the Shipping Line. This PIN number is unique to the Terminal Operator and supplements driver identification procedures.

Transmitting Pick-Up Information to Highway Carriers: Terminal Operator has created a secure transfer yard located on the outer perimeter of the port where inbound cargo from vessels is staged for pickup after inspection and clearance. As the loads are released for pickup, the information is transmitted to the Highway Carrier. Truckers must present documentation upon entry and are then permitted to enter the yard and pick up their pre-staged loads from designated locations. As drivers leave the yard, the guards verify the container, seal, and documentation against information in the computer database. A procedure to handle discrepancies has been established.

Warehouses/Factories

Establishing Driver Waiting Area: When the truck driver arrives at the Factory, he must have an appointment, ring a buzzer, and look into a camera. After the driver confirms his appointment, he is permitted to enter through a designated side door into a driver's reception area with a restroom. The driver must present the pickup order/delivery documentation and his driver's license. The driver's identity is verified against a drivers list with photographs that is provided by the carrier. A large sign is posted in the warehouse stating "NO VISITORS/DRIVERS BEYOND THIS POINT—EMPLOYEES ONLY." There is a gate between the warehouse and driver's waiting area. These controls help to prevent collusion.

Search Vehicles/Persons/Packages (Incoming)

Screening Incoming Packages: Company established an isolated area and procedures to screen incoming packages and mail before distribution. Company also uses the guidelines listed on the U.S. Postal Service's website to safely process incoming mail and packages. Each employee who is responsible for this function has been trained.

Randomly Inspecting Incoming Persons and Packages: A sign is posted notifying all who enter the Factory (including company managers and security guards), that a random search is conducted of incoming persons and packages. The Factory periodically conducts random searches of all persons and packages entering the facility. During periods of heightened security alerts, the Company inspects all persons and packages. Searches are documented.

Searching Lockers Prohibiting Personal Items: Personal bags are not allowed inside of the Factory and workers are provided with lockers separate from the Factory's production and warehouse areas. Lockers are periodically searched and employees are not permitted to access lockers during work hours.

Inspecting Vehicles: Terminal Operator's security personnel randomly inspect X% of all trucks entering the facility. A plan is established to randomly search X% of all private vehicles entering the facility each day. A log is maintained of all random inspections and management periodically reviews the log.

Challenging and Removing Unauthorized Persons

Responding to Unauthorized Access: The Company has the ability to lock down access points throughout the facility with the press of a button if unauthorized access is detected. There also is a "panic" button that triggers a silent alarm that will alert the guards and local law enforcement in case of an emergency.

Escalation Matrix: Company has an escalation matrix that has been communicated to all of its employees. The matrix shows the various levels of emergency contacts ranging from company management up to and including federal law enforcement. In addition, in-service training has been provided to employees on how to challenge and remove unauthorized persons.

Personnel Security

The purpose of conducting a background check is to ensure that a prospective employee is qualified to perform the job and is a person of integrity. Random background checks on current employees encourage good conduct. Poor hiring practices could result in security breaches, significant financial losses, and reduced productivity. Security breaches all have one thing in common…PEOPLE.

Pre-Employment Verifications, Background Checks, and Investigations

Domestic

Requiring Background Checks for Contracted Employees: Temporary employees, vendors, and contractors (such as security guards) are subject to the same background investigations required of the Company's permanent employees. The Company requests criminal background checks and application materials from vendors, temporary agencies, and contractors to ensure the integrity of persons having access to its facility and assets.

Conducting Comprehensive Investigations and Re-Investigations: Before hiring an employee, Company conducts in-depth criminal and background investigations for a ten-year period. These investigations include checking criminal records (local, state, and federal), court records, financial history, social security number, right to work documents, past employment, education records, and character references. In addition, employees who are promoted are subject to a reinvestigation. All other employees are subject to periodic reinvestigations.

Conducting Psychological Examinations: Prospective employees are administered a series of psychological examinations to determine their propensity toward corruption or illegal activities, as well as their ability to get along with others in the organization.

Verifying Authenticity of Identification: Human Resource Department verifies the authenticity of identification by using an I.D. Checking Guide that depicts driver's license designs from all over the United States and the world. The I.D. Checking Guide also is used to verify the authenticity of federal documents.

Foreign

Conducting Criminal Investigations in Foreign Country: A Factory and its Highway Carrier have contracted a private firm to run extensive criminal record checks to find individuals who have committed crimes in a foreign country. This background check supplements the requirement that prospective employees receive an original certification from the local police department attesting that they do not have a criminal record.

Employing Alternative Methods to Obtain Information: Although personal privacy laws exist in many domestic jurisdictions and various countries in which the International Company operates, the Company utilizes alternative methods to check applicants' backgrounds in instances where the

law prohibits criminal background checks. These alternative methods include asking probing yet noninvasive questions to stimulate conversation with the applicant including in-depth questions regarding gaps in employment; verifying an applicant's background by conducting in-depth personal reference checks and requesting additional references from those personal references; conducting personal visits to references and applicants' homes; verifying driving records (as relevant); verifying current and previous addresses; requesting educational transcripts directly from schools; and checking the applicant's reputation through local associations.

Conducting Criminal Investigations when not Customary: Background investigations are legal but are not customary in the Manufacturer's country. Therefore, all applicants must complete an "authorization to release information". The form authorizes the Manufacturer to conduct a criminal background investigation and obtain information regarding the applicant's character, general reputation, and mode of living. In addition, the Manufacturer obtains a release from current employees to conduct criminal background checks. These in-depth investigations are primarily performed on employees involved in international cargo handling such as shipping, sales/marketing, import/export, logistics, and finance, and personnel.

Personnel Termination Procedures

Establishing Employee Termination Procedures: Company has established employee termination procedures that are in writing. To ensure that termination procedures are consistently followed, managers/supervisors are trained on the employee termination process. A checklist is used to ensure that all access is terminated and that all Company property is retrieved. A final check will not be issued to the employee until all property is returned. Human Resource Management strictly oversees this process.

Handling Involuntary Separations: Prior planning is conducted with security and key management before involuntary separations are initiated. All facility access is terminated, keys and equipment are retrieved, and the employee is escorted out of the building. A list of names and photos of terminated employees are given to security guards to aid in the access control of the facility. An information notice is issued to all employees when an employee no longer works for the Company.

Internal Code of Conduct/Employee Evaluations

Addressing Security in Code of Conduct and Employee Evaluations: The Company's Code of Conduct specifies the type of disciplinary action taken when employees violate company security. In addition, the Company includes security as part of its employees' job descriptions and annual performance reviews.

Procedural Security

Security measures must be in place to ensure the integrity of the supply chain. Regardless of a company's size, written policies are needed to achieve effective supply chain security. Procedural security requires oversight, accountability, control, and a system of checks and balances. Technology should be used to enhance all aspects of procedural security.

Identifying/Reporting/Tracking Incidents

Brokers

Maintaining Incident Database: Broker has a central "Security Incident Database" that records all incidents such as overages and shortages. Senior management monitors the database to identify trends or patterns that might reveal a potential security risk within the supply chain.

Identifying Suspicious Activity: Broker developed a list of "suspicious activity" indicators and trained employees on what to look for and how to report such activities to management and CBP.

Addressing Unexplained/Unusual Delays: Broker keeps track of inbound shipments. Unusual or unexplained delays are referred to CBP and a courtesy examination is requested.

Carriers

Establishing Written Procedures to Handle Suspicious Activities: Highway Carrier has established a written procedure to identify suspicious shipments by examining documents, observing unusual behaviors or requests, and monitoring activities at pickup locations. The procedure specifies whom to contact, up to and including CBP.

Establishing Global Reporting and Incident Response Procedures: International Logistics Provider has taken steps to globalize security procedures and reporting. The Security Department developed written policies and procedures to ensure that an efficient and reliable system is in place to report, document and analyze incidents. The Security Department investigates serious incidents, and coordinates with management, local law enforcement, and CBP to resolve issues and improve security. The procedures are reviewed and updated by the Security Department as business practices change.

Assessing Customer Risk: Air Carrier uses a database that tracks cargo and maintains information on the status of shippers. Air Carrier's agents use an information database to determine if the freight will be accepted for processing on passenger flights. Risk indicators are built into the system to perform this analysis. After cargo information is input and a customer's name appears as a "do not load," the cargo will not be accepted. This system allows the Air Carrier to instantly pass on information about high-risk customers to CBP and other law enforcement agencies.

Brand Name/Identity Protection

Safeguarding Company Stationery: Company safeguards forms and stationery by controlling their issuance and securing them in a locked cabinet in an office where access is controlled. A designated company supervisor controls issuance of forms, and the forms are strategically numbered to detect unauthorized use. In addition, the Company's stationery bears a watermark to prevent unauthorized duplication.

Safeguarding Items Bearing Company Logo: Stamps, tape, and cartons bearing the Company's logo are controlled and their use is monitored. Stamps and tape are issued only to employees who are authorized to use them and are secured while not in use. Cartons are counted, and logos on recycled cartons must be obliterated.

Destroying Sensitive Documents: Sensitive documents are shredded when no longer needed. The Company's representative supervises a contractor to ensure that none of these documents leave the premises without being shredded.

Archiving Records: Archived records are secured in a caged area of the warehouse. The warehouse supervisor controls access to the archives and only authorized employees are permitted to enter this area.

Securing Business Documents : All business documents, including purchase orders, invoices, manifests, and customer information are kept under lock and key when the Company is not operating. Employees are required to secure documentation prior to leaving for the day.

Manifesting/Invoicing/Electronic Data Interface (EDI)

Receiving

Domestic Distribution Center

Utilizing Radio Frequency Identification (RFID): RFID technology is used by the Domestic Distribution Center to obtain "real-time" information on the flow of cargo and enables the Center to immediately address inventory discrepancies. In addition, manifest, invoice, inventory, and packing information are electronically transmitted to the Distribution Center's inventory and accounting systems for cross-checking.

Establishing Automated Import Tracking System: Company has established an in-house automated import tracking system. Once the booking is received from the consolidator, it is uploaded into the Company's tracking system. This allows the cargo to be tracked and verified within the shipping, receiving, and traffic departments. Information includes the factory name, container number, seal number, bill of lading number, estimated date of arrival, quantity and weight of merchandise.

Restricting Access to Documentation: Limited access to Electronic Data Interchange (EDI) has enabled the Company to ensure document security and has eliminated data input duplication. The

use of EDI reduces clerical errors and the opportunity to manipulate or alter data. Transactions are traced through user identification numbers.

Shipping

Consolidator

Ensuring Only Manifested Cargo is Loaded: Consolidator ensures that only properly marked and labeled cargo is loaded. The Consolidator electronically scans each unit prior to placement in the shipping container. A cross-check is conducted in the computer system at the end of loading to ensure that only manifested cargo is shipped.

Factory/Shipper

Transmitting Advanced Information to Company: Shipper generates documents after stuffing the container and transmits all packing, invoice, container, and seal number information to its customer via Electronic Data Interchange (EDI). An e-mail containing this information also is sent to the customer confirming the details of the shipment. Once received, the customer verifies the shipment before the cargo leaves the shipper's premises.

Weighing Product: For each product, the Factory has a preestablished weight and each package is bar coded for inventory tracking. The product is weighed several times during the production and packing process. If the weight exceeds or is significantly less than the preestablished weight, the system will issue an alert prompting Factory officials to remove the product and investigate the cause of the weight variance.

Restricting Access to Cargo: After the Factory packages the goods for export, they are staged in a highly secure fenced area in the warehouse where access is restricted. At the time of container stuffing, the warehouse manager, shipping supervisor, and a security guard are present; each have backups when absent. Responsible parties must sign-off on the security "check sheet." The Factory General Manager reviews this "check sheet" daily.

Verifying Inspection, Seal, and Manifest Upon Departure: Factory does not allow the truck driver to leave the factory until exit procedures are followed which include the issuance of a signed "exit pass" by the shipping department. The "exit pass" can only be signed-off by a limited number of shipping managers and must be verified by security personnel. The "exit pass" is used to verify that the container was inspected, the cargo was loaded, and that the seal and trailer numbers are correct.

Freight Forwarder

Establishing Booking and Manifesting Procedures: A detailed Standard Operating Procedure (SOP) exists between the Freight Forwarder and the Shipper in accordance with their service agreement. The SOP details how to make a booking, what personnel are authorized to make a booking, manifesting requirements, discrepancy reporting, protocol for making changes, and other essential information to ensure the accuracy and security of cargo information.

Air Carrier

Limiting Cargo Hold Time: Air Cargo Consolidator minimizes the time cargo is maintained in the warehouse by matching the schedule of delivery trucks with aircraft departure times to limit the amount of time available to tamper with cargo.

Sea Carrier

Establishing System of Checks and Balances: Sea Carrier has a system of checks and balances to ensure the accuracy of its shipping information. For example, the container number in the automated documentation system is reconciled against the container records in the equipment system, and the stowage plan is reconciled against the equipment and container records.

Packing/Packaging

Utilizing Special Packaging Material: Factory uses a special compressed packaging material that once opened, cannot be repacked.

Specialized Packaging: Factory seals each carton with tape that has the Factory's name imprinted on it. In addition, each pallet is color-coded shrink wrapped, stamped with the Company's seal (that is controlled by the shipping manager) and labeled with the Factory's and Consignee's names. The label is clearly visible from a distance and also contains a barcode with packing and shipping information that is readable using a hand held barcode scanner. Barcode scanners may only be used by authorized personnel and are stored in a secure location when not in use.

Factory

Unique Shipping Mark: A unique shipping mark is generated for each purchase order that gives the shipper, logistics provider, and consignee the ability to verify that each shipment is legitimate. The shipping mark serves as an additional safeguard to ensure that no unauthorized cargo has been introduced into the shipment. If a carton has an incorrect or missing shipping mark, it is rejected and immediately investigated. The same shipping mark is never used twice.

Employing Anonymous Observers: Company employs "anonymous" observers who are considered regular employees in the packing and shipping departments. The immediate supervisors of these employees are unaware that they report directly to company executive management.

Conducting Random Inspections: Factory conducts random documented examinations of cartons prior to palletizing. After cartons are examined, they are stamped with an "EXAMINATION" stamp, and resealed with tape bearing the Factory's logo. The cartons are then palletized and shrink wrapped.

Cargo Discrepancies

Bar Coding and Scanning to Reduce Cargo Discrepancies: Company utilizes a bar code/scan and pack system. This system allows overseas vendors to electronically transmit shipping informa-

tion including packing list data to the Company's distribution center. The barcode system ensures product accountability from the time of packing until its delivery to the distribution center in the United States. This system has reduced the number of quantity discrepancies experienced by the Company's distribution center.

Weighing Contents: Factory uses a computerized line production system that generates an itemized record of the contents of each box. The weight of each item is recorded and transmitted to the distribution center in the United States. Each carton's weight is checked at various stages throughout the supply chain. Weight discrepancies are flagged by the system and investigated.

Preventing Collusion

Rotating Dispatchers and Customer Assignments: Each dispatcher is assigned a specific set of customers so that he can become familiar with customer and cargo movements to identify anomalies. Assignments are periodically rotated to prevent collusion.

Rotating Shipping/Receiving Personnel: Factory periodically rotates shipping, receiving, and inventory management personnel in order to prevent collusion.

Security Training/Threat Awareness/Outreach

The tragic events of September 11, 2001 and other terrorist acts were well planned, organized, and carried out by individuals or groups. Some of the precursors include conducting surveillance, eliciting information, testing security, obtaining supplies, conducting trial runs, and deploying assets/getting into position. A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of a threat posed by terrorists at each point of the supply chain. Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail

Awareness

Initial and Periodic Training: Company has integrated security training into its new employee orientation and periodic refresher training is given to existing employees.

Using Alert Levels: Company provides employees with information received from government alerts to ensure that they are aware of the current security alerts. Company then adjusts its alert levels to coincide with those of Homeland Security.

Communicating Terrorism Information to Employees: Company created a terrorism information bulletin board where its employees can view photographs of terrorists and the latest information on terrorist activities throughout the world.

Training Video: Terminal Operator has created a training video that illustrates the techniques used to breach containers. This video has raised security awareness throughout the trade community.

Online Security Courses: Sea Carrier has a mandatory security awareness program for its employees and has developed a course on how to recognize internal conspiracies, maintain cargo integrity, and spot unauthorized facility access. This training consists of a series of online courses where the employees' enrollment and completion are recorded. The Carrier's security department ensures that all employees complete this course and generates a report that details the completion status of every employee.

Intranet and Company Magazine: Highway Carrier has established a formal security-training course and has set-up its own intranet "University" to train drivers on theft, security and terrorism issues. Company also publishes a magazine to address new policies and security requirements, as well as commend employees for positive work contributions. All training is documented by department supervisors and is periodically reviewed to ensure all employees have been trained.

Continuing Education: Highway Carrier management keeps abreast of the latest cargo security procedures and technology by reading periodicals and attending security conferences. Information acquired is passed on to employees to keep them up-to-date on global security issues. A system of accountability ensures information is passed on to employees.

Specialized Training

Training in Areas of Specialty: Employees must complete mandatory training courses that focus on their area of specialty. Training coincides with changes within the global supply chain, including trade lanes used. Company requires all employees to take antiterrorism courses. Attendance is documented in an automated system to facilitate supervisory reviews and identify employees who have not been trained.

Product Tampering, Collusion, Loss Prevention, Handling Breaches: All employees at the Company's foreign factories, shippers, and service providers have been provided with seminars on such subjects as product tampering and smuggling, methods to prevent and detect collusion, the importance loss prevention policies, effective response techniques, and how to report and handle security breaches.

Conducting Background Investigations: Employees in the Human Resource Management Office receive specialized training on how to conduct employment, reference, driving record, education verifications, and criminal background investigations. In addition, specialized training is given to human resource employees on how to spot fraudulent documents, verify work eligibility, and investigate gaps in employment. They also are trained on techniques to illicit information from applicants without appearing invasive or rude.

Segregating and Reporting Suspicious Containers: Company has trained its personnel to profile container appearance and conditions. If anything suspicious is detected, the container must be segregated into a designated "safe and secure" area. A reporting procedure is in place to contact company management, local law enforcement, and CBP when anomalies are identified.

Conducting 14-Point Trailer and Conveyance Inspections: Highway Carrier has trained all drivers in a 14-point conveyance and trailer/container inspection. Drivers are trained to document inspections and immediately report discrepancies and anomalies to company management, local law enforcement, or CBP, as appropriate.

Highway Watch: Highway Carrier requires every driver to participate in the Highway Watch security orientation and training sponsored by the Department of Transportation and Department of Homeland Security. Highway Watch trains drivers to identify and report suspicious activities while on the highway.

Utilizing External Resources: Highway Carrier invites a private security representative to attend monthly meetings with drivers. The security representative briefs drivers on the latest schemes used by smugglers and how to avoid getting involved with suspicious people and companies.

Security Guards: Security Guards are professionally trained to immediately identify, confront and report any situations of unauthorized access or other unusual activities; perform patrols; use self-defense techniques, and exercise emergency/crisis management. Specialized training includes: CCTV monitoring techniques, non-lethal weapons training, and methods terrorists use to infiltrate legitimate businesses. Guards are required to receive periodic specialized training to maintain

their state issued "Guard Card". The Chief of Security oversees the training, education, and awareness for the facility's guards.

Dual-Use Awareness: Chemical Factory formally trains its sales representatives, drivers, and shipping personnel to identify terrorist threats. This training covers indicators of suspicious activities such as large orders of chemicals by unknown customers or unusual requests by known customers

Outreach

Collaborating with Local Law Enforcement: Company works closely with local law enforcement and other businesses to maintain an awareness of criminal activities.

Training Business Partners: Foreign manufacturers, suppliers, and service providers are given formal onsite supply chain security training sponsored by the U.S. Company to ensure that supply chain security expectations are fully understood and met. This training is documented and participants are tested to ensure their understanding of the information taught.

Translating Training into Multiple Languages: International Logistics Provider has published their security policies and procedures on the intranet. Security policies and procedures have been translated into several languages. A computer-based reference library allows immediate access to corporate policies and procedures concerning security. In addition, employees are given periodic security training via the intranet. Supervisors are required to review and follow-up if necessary. Some training focuses on "general security awareness" while other training is specifically tailored to key areas such as container and transportation security.

Receiving Updates From Association: Highway Carrier receives continual security updates from its association and provides information to its drivers regarding hazards and security risks.

Employee Incentives

Providing Incentives: Company has incorporated into security into its "Business Improvement" incentive program. Employees are given incentives for reporting security anomalies and recommending ways to improve the Company's security.

Incident Reporting

Establishing a Hotline: Company implemented a 24/7 anonymous "hotline" that is available to all employees and vendors (globally) to report suspicious or criminal conduct within the organization, as well as questionable business ethics.

Outsourcing Hotline: The Company's incident reporting hotline is outsourced to a third party so employees are assured of anonymity. In addition, there are posters displayed throughout the facility and handouts regarding reporting procedures are distributed to employees.

Issuing Emergency Contact Information: Highway Carrier has given each driver a card that lists company emergency contact phone numbers, including the CBP FAST Office, and the CBP hotline 1-800-BE-ALERT.

Issuing Business Integrity Cards: Company issues business integrity cards to all associates worldwide. The cards provide contact information and instructions for employees to discreetly report suspicious activities and security violating to the corporate security staff and terrorist threats to CBP via 1-800-BE-ALERT.

Physical Security

The physical security of a facility is its first line of defense from intruders. In particular, cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access.

Fencing/Gates/Gate Houses

Secure Loading: The factory has a caged area that encloses the top and side of the truck in order to restrict access to the truck during loading. The caged area is locked when not in use. Signs posted stating "restricted access" are placed on the fence and a guard is present to ensure no unauthorized people approach the truck as it is being loaded.

Magnetic Sensors: The fence surrounding the cargo handling and storage area is equipped with magnetic sensors that are activated if pressure is applied.

Controlling Gate Access: Company issues a time-controlled exit card for departing truckers to ensure compliance with loading and unloading intervals.

Utilizing Technology to Monitor Gates: Company's foreign facilities have electronic gates, perimeter fences with infrared and magnetic sensors, motion detectors, and alarms.

Security Guards

Equipping Security Guards with Adequate Resources and Orders: Guards are given appropriate uniforms and equipment for their work environment (e.g., communication devices with appropriate range, self-defense gear, search equipment, etc.). Post orders/standard operating procedures exist, are periodically updated, and are clearly defined. Guards have a clear understanding of the organization, receive site-specific training, and are familiar with the facility's physical layout, security features, and vulnerabilities. Security Guards are periodically rotated to prevent collusion and predictability.

Procedures for Selecting Contracted Security Guard Services: A comprehensive plan exists when selecting contracted security guard services. The plan includes evaluating the service provider's selection, training, and supervision of the guards.

Supervising Contracted Security Guards: A Company manager has overall responsibility and supervision for both Company and contracted security guard services, including review of guards' performance, daily patrol logs, and adherence to post orders and patrol schedules.

Ensuring Shift Coverage and Accountability: Guards' shifts overlap to provide a briefing period; periodic meetings are held with guards to discuss facility security and alerts. Company management conducts routine verifications of guards' performance on all shifts.

Establishing Patrols: Company has a system that is based on random checkpoints. It establishes critical checkpoints throughout the facility. Security personnel are given several different routes that change randomly. This system helps to decrease guards' predictability.

Preparing and Reviewing Reports: Company's security guards prepare security reports on all three shifts. The reports include the name of the security officer on duty, hours worked, areas patrolled, and the time areas were patrolled. The report also includes unusual incidents that do not appear to be suspicious on the surface (e.g., company truck broke down, driver had to take to shop). The Security Director reviews all security reports and uses them to identify security breaches or other unusual events that may be a pre-cursor to a security incident.

Parking

Procedures for Issuing Parking: Employees have decals on their cars to determine which vehicles belong to employees. Employees must obtain a temporary parking pass if they do not have their decal. Company maintains a list of all decals issued, including decal number, employee name, department, vehicle make and model, department, etc. Lost or stolen decals must be reported.

Locking Mechanisms

Changing Locks: Keys are only issued to individuals who have a need to access the facility or designated area. Issuance of keys is recorded and controlled. If an employee no longer works in a particular area, his key is retrieved. If a key is lost, misplaced or stolen, it must be reported immediately and the lock is changed. Periodic inventory of keys is conducted to ensure none have been lost or misplaced.

Lighting

Verifying Functionality of Lighting: Company has a procedure to immediately replace lights that burn out. Company conducted a survey of the facility's interior and exterior lighting to ensure uniformity and appropriate brightness for the facility's size and operations. Company has designated personnel who routinely visit the facility at night to identify which areas an intruder would attempt to enter. Company also consulted with the local police department on appropriate facility lighting.

Alarm Systems

Configuring Alarms: Alarm zones were carefully configured to maximize their effectiveness. Company identified areas of greatest traffic, vulnerability, and use and worked with security specialists to select an appropriate alarm system. Company's alarm system is equipped with a cell phone backup.

Utilizing Long Range Sensors: The cargo warehouse is protected with an alarm system that is equipped with several sets of long-range infrared sensors. A set of infrared sensors includes both functional and redundant sensors to ensure a backup in case of failure.

Assigning Individual Deactivation Codes: Codes to deactivate the building's alarm system are individually assigned and restricted to those with a need to have access to the building. Company management keeps track of the assigned codes. Company will periodically review reports to identify patterns of unusual access and immediately deactivate codes when an employee is terminated.

Monitoring Exits: All exits from the facility are equipped with an alarm system that is monitored. If the doors are opened without proper card key access or propped open for a period of time, an alarm will sound and the guards will immediately respond.

Video Surveillance Cameras

Storing Recordings: Video surveillance recordings are maintained for a minimum of 30 days and are stored in a secure location with restricted access. Management periodically reviews the recordings.

Maximizing Recording: The digital video surveillance cameras adjust to night lighting, are motion activated, and record high quality images to ensure their usefulness when conducting investigations.

Detecting Intruders: Terminal Operator has a digital video surveillance system that will record anyone who attempts to access a restricted area. The video surveillance system will capture the intruder's image and send it to the security database for immediate response by the guard. The system is equipped with cameras that will record intruders as they set off an alarm or as they move through the area.

Monitoring, Maintaining, and Upgrading System: Port has a surveillance camera system that is staffed 24/7 by security officers. The system features high resolution of key areas so that potential breaches can be identified and recorded with great clarity. All images are projected on wall mounted plasma screens and the camera control panels are situated in conjunction with the communications and dispatch system. This comprehensive system ensures problems are handled expeditiously and efficiently. The system is continually upgraded and expanded. Fiber-optic capability and motion detectors are deployed throughout the Port.

Remote Monitoring: Company senior managers have remote Internet access capability to view recorded activity captured on the video surveillance camera system. In addition, Company also provides the local police department with this capability.

Strategic Placement: Company has several video surveillance security cameras strategically located throughout the facility, including at the loading docks, cargo handling/storage areas, and at facility entrances and exits. These cameras have telescopic and night vision capability. Some exterior cameras have the capability to scan the entire property. Security personnel and company management monitor the cameras.

Information Technology Security — Computer Systems

Access Restrictions (Internal)

Changing Passwords: Individual passwords are used which consist of a combination of letters, numbers, and symbols that cannot be personal identifiers. Passwords must be changed at least every 90 days, cannot be reused, and are deactivated if the password is not changed. An alert message is generated a predetermined number of days before the password expires.

System Lock Out: All users have a login code, station number and password to access the system. After three unsuccessful attempts to login, the user is locked out of the system and the IT administrator, with the authorization of the user's supervisor, must reinstate the user's access to the system.

Monitoring and Limiting Internet Access: Company limits the number of employees that can access the Internet and requires that they sign an agreement that outlines system security requirements and site access restrictions when using the Internet. Company has software to track Internet usage and is able to identify abuse.

Establishing and Reviewing Access Levels: Levels of access to the computer system are assigned by job category and established by the corporate office. Access levels are reviewed when there is a job change within the organization. In addition, management periodically evaluates access levels of current users and will change access levels as job responsibilities change.

Temporary Access Suspension: During an employee's extended absence (e.g., disability), access to the information system is suspended until their return.

Viruses/Firewalls/Tampering Prevention (External)

Maintaining System Integrity: Company's IT system contains multilevel safeguards, allowing the system to both log and detect viruses, security violations, and tampering. This system allows the IT department to identify weaknesses and initiate efforts to safeguard the Company's IT systems worldwide.

Educating Employees on System Vulnerabilities: IT personnel maintain a constant awareness of cyber attacks and counterattacks that are occurring with automated systems throughout many industries to ensure the Company's system is protected from a breach. Alerts are given to system users to prevent virus attacks and improper release of information.

Utilizes Data Encryption: Wireless communication devices use state-of-the art data encryption technology to prevent unauthorized system access.

Virus Quarantine Software: Company has a "virus quarantine" software program to view file content, origin, and type of virus without infecting the rest of the system.

Securing Remote Access: Company implemented a Virtual Private Network (VPN) for users to communicate within the Company. Each employee that has access to the VPN is issued an access card and unique PIN number. The access card has a random sequence of numbers that changes every minute in order to protect the system from unauthorized access.

Testing System Security: Company contracted a reputable, highly qualified, thoroughly screened service provider to hack its computer system in order to identify vulnerabilities and weaknesses.

Policies/Procedures/Management Support/Training

Comprehensive Approach to IT Security: Company regularly holds meetings that are attended by senior management to address information technology issues, including system security. Company has conducted a thorough analysis of system vulnerabilities; developed a data recovery plan; routinely identifies and responds to virus threats with the most up-to-date anti-virus software; and trains employees in information system security principles and data integrity. The IT security policy is fully documented and addresses access controls and system protection. Updates are communicated to employees. Employees are required to take a basic security awareness course for IT. Company fully supports the continuing education of its IT workers and gives them the opportunity to attend specialized training and conferences to keep up-to-date on information technology security.

Data Back-Ups and Recovery Plans

Contingency Planning: Company has a contingency plan to protect its IT systems, which include a full IT disaster recovery plan to prepare for any unforeseen incidents. It also utilizes Uninterruptible Power Supplies (UPS) for power surges/failure.

Data Storage: Company conducts system back-ups daily that are stored in a safe that is fireproof and only accessible to the IT Manager and senior company executives. Additional back-ups are stored off-site weekly with a bonded company.

Hardware Security

Controlling Workstation: Employees are required to swipe their ID card and enter a password before they can use their workstation.

Securing Server: System server is stored in a fireproof locked room where access is restricted and tracked.

Password Protected Screen Savers: Employees are required to use password-protected screensavers on their workstations. Screensavers must be activated when employees leave their workstations. Screensavers are automatically activated within a specific period of time when there is no activity at the workstation.

Emergency Preparedness/Disaster Recovery

Emergency Generators: Factory has a disaster recovery plan that includes an emergency generator for back-up power to ensure security systems continue to work.

Disaster Plan: Company has a disaster plan to ensure the continuity of its operations in the event of a man-made or natural disaster. The plan includes mock-disaster exercises to ensure employees are well prepared and the plan is kept up-to-date as organizational changes occur.

Building Evacuations: In the event of a building evacuation, a plan has been established whereby security personnel and management are assigned by section to account for employees and visitors and conduct an "area sweep" of work locations and restrooms to ensure that all areas are secured in the event that the alarm was falsely initiated. Security also verifies that all computers are logged-out or password protected screensavers have been activated.

Alert Levels: Company developed a threat level response system consisting of three-tiers. Each threat level (low, medium and high) has a specific set of security measures. Threat levels are communicated to staff by management so that all personnel can respond accordingly.

Supply Chain Continuity Plan: Company developed a "Supply Chain Continuity Plan" which consists of policies and procedures to handle a variety of disasters or a terrorist incident; identify the potential impact of a disaster/terrorist incident on supply chain security; conduct mock incident exercises to ensure staff preparedness; and collaborate with government entities, supply chain partners, and industry colleagues.

Program Memberships/Certifications to Enhance Supply Chain Security

Government/Industry Partnership: Company is a member of a foreign government's industry supply chain security partnership program.

Associations: Company is actively involved in promoting supply chain security through its professional association and has encouraged others in the industry to become actively engaged.

Business Certifications: Company has business certifications that support and enhance supply chain security efforts.

U.S. Customs and Border Protection
Office of Field Operations/C-TPAT
Room 5.2C
1300 Pennsylvania Avenue, NW
Washington, DC 20229

www.cbp.gov

January 2006