C-TPAT Best Practices Catalog Addendum 2009

TABLE OF CONTENTS

.

Introduction to Best Practices

In 2006 C-TPAT published the first *Best Practices Catalog* in an effort to provide members with up to date information regarding highly effective cargo security practices identified while conducting validations. Since then C-TPAT has conducted more than 8000 validations and revalidations throughout the world and clearly security processes have improved and evolved over time. This supplement identifies innovative solutions developed by C-TPAT members to comply with the minimum security criteria.
Best Practices are generally defined as supply chain security measures that:

1) Exceed the C-TPAT minimum security criteria
2) Incorporate senior management support
3) Have written and verifiable process that govern their use
4) Employ a system of checks and balances
5) Have measures in place to ensure continuity

This addendum is written in a generic manner to allow for flexibility while maintaining the confidentiality of C-TPAT partners and preventing the endorsement of specific technology, services, or products. To provide context we have identified the business entity type e.g. Company, Highway Carrier, Importer, Foreign Consolidator in which the best practice was identified. Best practices listed in this addendum and the original catalog are not necessarily exclusive to the entity mentioned and are applicable to many supply chains. For example, a physical security best practice described as being performed by a foreign manufacturer may also apply to an importer.

Best Practices are achieved through the effective utilization of people, processes and available technology. They incorporate a system of checks and balances, high level managerial oversight, accountability, and verification of reliability to ensure that a company's international supply chain cannot be compromised. While many of the best practices listed in this addendum may help businesses in theft prevention and asset protection, their intended use here focuses on the prevention of weapons of mass effect, terrorists, and/or contraband from entering the international supply chain.

This addendum is not exhaustive or all-inclusive of all the best practices present in the thousands of C-TPAT partners' international supply chains. It is intended to serve as a living document which is periodically updated to reflect the best practices found during validations and revalidations. In addition, this addendum and the original Best Practices Catalog are not designed to function as a "master check list" of security practices. The C-TPAT program from its inception has taken a flexible approach to supply chain security. It is recognized that "one size does not fit all" and that customized security measures have been developed and implemented to address each partner's risk assessment. It is also important to remember that a single best practice does not constitute an effective supply chain.

My thanks to all of the C-TPAT companies and their business partners who have developed new and innovative ways to secure the international supply chain through the implementation of the best practices identified in this document.

Bradd M. Skinner
Director, C-TPAT/Industry Partnership Programs
Office of Field Operations
U.S. Customs and Border Protection

Risk Assessment

The Importer has adopted a computer software risk-based assessment tool. The use of this program allows the company to analyze and identify critical areas of its international supply chain that are the most likely targets for infiltration.

The Importer has created an extensive "Facility Performance Manual", which management uses to grade its suppliers supply chain security criteria. Upon completion of a security audit by management, a grade of 0-100 is assigned to the facility: "Probation", "Authorized", "Excellent" or "Business Partner". If a facility's score correlates to "Probation" status, the facility will have two weeks to provide a corrective action report and a follow-up audit will be conducted. If the follow-up audit does not result in a score correlating to "Authorized" status, the contract with the Importer will be terminated. If a facility's score correlates to "Excellent" status, it receives a certificate from the president of the Importer and if a facility's score corresponds to "Business Partner" status a "Business Partner Award" plaque and a $5,000 reward will be given to the facility.

The Company has written processes for the selection of their business partners to include a detailed risk assessment software system called the Supplier Business Engagement Model (SBEM). This strategy focuses on managing and recognizing the supplier's products, software and services. The process includes various site visits made annually. The SBEM Model includes a six step process: • Conduct Supplier Evaluation • New Supplier Assessment, Approval and Coding • Product/Material/Component Qualification and Coding • Supply Agreement Process that includes a review board • Complex/Product/Application Approval/Functional Verification (New Product Introduction or First Piece Evaluation) • Relationship Management (On-going monitoring & verification)

The Company has implemented a three tier internal audit system. A Tier One audit of the company's security and safety procedures is conducted on a monthly basis. A Tier Two audit is conducted every two months to serve as a more comprehensive security audit of all the Company security policies and procedures. A Tier Three audit is a Company wide check on all of the Company's security policies, process and procedures. This audit also includes all security measures used to secure the company's international supply chain. Each tier audit is documented and executed according to the company's standard operating procedure (SOP).

Business Partner Requirements

The Company's C-TPAT liaison personnel (full-time employees dedicated to C-TPAT compliance) conduct supply chain security audits to ensure compliance of their non-C-TPAT business partners.

An outside security agency hired by an Importer conducts security audits of the Foreign Manufacturer's warehouse without advance notice. If sufficient cause exists, based on non-compliance or suspicious activity, the outside security agency has the authority to have the facility cease loading operations and prevent freight from boarding aircraft at the foreign airport.

An Importer's foreign manufacturer has created a full-time dedicated Director of Responsible Care Coordination, who is responsible for conducting and coordinating security self-assessments. The self-assessments include reviews and audits of security procedures, physical security, and security training.

An Importer's foreign manufacturer is certified as an "Authorized Exporter" by the Ministry of Finance (MOF). MOF conducts onsite inspections and verifications to ensure that the freight is secure and that the exporter is following security processes.

The Importer only ships cargo through CSI ports. The Importer also only uses steamship lines that are C-TPAT certified.

An Importer has created a Facility Status Tracking Log to monitor the compliance of all its North American manufacturing facilities. An "easy-to-read" spreadsheet incorporates all C-TPAT security criteria and designates risk-level (based on cargo volume and product source country) at each facility. The company's C-TPAT task force and executive managers review the spreadsheet monthly to identify any new security threats.

The Importer has developed a "Three Audit Rule", for its foreign manufacturing companies. If a foreign manufacturer is identified as having a security violation, the company is issued a letter that identifies security discrepancies. A corrective action letter is also sent to the factory to give management the opportunity to correct the deficiency. If the deficiency is not remedied by the third visit, the Foreign Manufacturer's contract with the Importer is terminated.

The Importer has established a C-TPAT Program Management Team consisting of a dedicated internal panel of managers who direct the company's security efforts and involvement in the C-TPAT Program. To ensure its supply chains from foreign source points are secured, the company has established and maintains numerous supply chain inspection offices in foreign countries where they conduct business.

The Company’s supply chain management buyers are required to screen all procurements, regardless of dollar amount, for supplier debarment or ineligible status using the Company's restricted party screening tool. This computer-based program includes the U.S. General Services Administration "List of Parties Excluded from Federal Procurement and Nonprocurement Programs" as well as other known sanctioned party lists (e.g. Terrorist List, Specially Designed Nationals, Denied Parties, etc.).

When performing periodic audits of their business partners, the Importer utilizes a third-party security company that joins them on the site visits. The contract security company is tasked with making specific observations as they relate to the security criteria in the C-TPAT program. The third-party company submits written reports of their findings to the Importer’s senior management. Management carefully reviews all audit reports and potential security weaknesses are immediately addressed. The information contained in these reports is made available in advance to C-TPAT validation teams.

The Importer’s security department distributes an operational audit report several times throughout the year. Each of the Importer’s domestic and foreign manufacturing facilities has an audit completed of their internal security processes each year. A numerical security assessment score is generated for each facility worldwide. If the score is lower then a minimum requirement, the Importer’s security department determines the facility’s security weaknesses and starts corrective actions.

Conveyance/Container/Trailer Security

High security seals are considered to be company property by the Importer, not an expendable item. All seals are logged into the foreign supplier's inventory control system.

The Highway Carrier's global positioning system (GPS) is equipped with the capability to detect when the engines of the company's vehicles have been shut off, or if the door of the conveyance has been opened. As an added security measure, the company's security manager remotely disables the engines of all conveyances not in use between 8:00 pm and 6:00 am through the GPS system.

The Importer maintains two colors of ISO/PAS 17712 seals (blue & yellow) that coincide with the ultimate consignee's relationship with the foreign manufacturing facility. Blue-colored seals, bearing the company name, are used if the shipment is consigned to another company-owned entity and yellow-colored seals are affixed to the intermodal container if it is destined for a third party such as an independent distributor.

All empty containers are stored at a Foreign Manufacturer's loading docks. The dock doors are equipped with infrared sensors to detect any unauthorized access to the container doors. In addition, all empty containers are also kept sealed at all times.

An Importer's foreign manufacturer affixes labels on export freight that bear a special code. The unique code identifies the shipments to a contracted security firm's personnel at the foreign airport loading site.

An Importer has produced a seal change form that accompanies the bill of lading and invoice for each shipment destined to the U.S. This form is written in French and English and is required to be used to document all seal changes that occur while a shipment is in transit to the U.S.

The Importer requires that all arriving cargo from foreign locations is delivered by authorized Company drivers and must be scanned by company-owned radiation detectors prior to unloading.

The Importer requires that all containers it uses are never used by any other company and are always sealed except during loading in Japan and unloading in the United States.

The Importer requires that its Foreign Manufacturers ship service parts directly to the U.S. using C-TPAT carriers in full container loads only. No foreign consolidators are used in the loading process.

An Importer utilizes metal racks for shipping its products from foreign locations to the U.S. These racks are sized specifically to fit into the ocean containers. Any anomaly within the container, such as a false wall, ceiling or floor, would prohibit the metal racks from fitting within the container and would alert those loading that the container may have been altered.

A Foreign Manufacturer utilizes a progress control board to monitor the status of up to 230 trucks per day. The progress control board is a simple and highly effective magnetized grid board that has color-coded magnets which show the appointment times and status of each incoming delivery for the day. There is a written procedure in place to identify/inquire if trucks are late for their appointment at the Foreign Manufacturer. The board is checked every hour and if a truck is over 30 minutes late, then the Foreign Manufacturer notifies the Highway Carrier of the discrepancy.

The Importer's containers are laden onto vessels via a private section of an internationally recognized steamship line. The steamship line is C-TPAT certified. A private berth is used in the foreign port of lading to load the Importer's containers. The private berth is controlled by three steamship lines which are all C-TPAT certified carriers.

The Importer requires that a "Declaration of Security" regarding laden cargo be signed by both the ship captain and the foreign port facility before any containers are loaded onto the vessel. This declaration certifies that containers have been inspected for anomalies.

An Importer has used its leverage with shipping lines by requiring ocean carriers to provide "seaworthy" containers at all times. The Importer requests that containers dispatched from the steamship line be less than five years old. This policy enables the Importer to easily perform container inspections, since newer containers are less likely to have had repairs or modifications made to them.

On inbound refrigerated containers the Importer uses in-transit temperature data sensors to ensure product quality. The data sensors are integrated into the Importer's computer software and if a refrigerated container's door is opened in-transit, it activates an electronic alarm.

The Importer's container storage area is enclosed by a 20 ft. concrete wall. The high walls prevent viewing inside critical cargo and handling areas by outside parties.

To increase cargo security, all of the Importers shipments undergo Non-Intrusive Inspection (NII) prior to loading on a vessel in a foreign port. Radiation Portal Monitors (RPM) are used to measure nuclear and radiological levels in cargo and the Company has written procedures in place to address any anomalies.

The Importer requires that containers have four separate inspections conducted in the foreign country in accordance with written checklists. Each checklist contains the recommended C-TPAT seven-point inspection. The first inspection of an empty container is conducted at the vessel carrier's yard. The empty container is sealed by an Importer's representative immediately after the inspection and the corresponding seal number is communicated to the security center at the foreign manufacturing facility for verification upon arrival. The second inspection is conducted at the foreign manufacturing facility's main gate by security guards. A third inspection is conducted at the facility weight scales. The final documented inspection is conducted by shipping personnel before loading begins. All checklists are maintained on file by the Foreign Manufacturer.

The Importer requires that five security devices are used on each container destined for the U.S. An ISO/PAS 17712 certified cable seal, two hinge tapes, one bolt seal, and an electronic seal are used on each container destined to the U.S.

The Steamship Terminal's operational facility contains an automated container yard. Cranes are utilized to pick up each container; once the container is attached to the crane the operator pushes a button that activates the automated process. The automated system controls the stacking of the containers and these boxes are randomly assigned a spot in the 22-stack block. This feature makes it virtually impossible for an individual to know the exact location of a container.

The Importer has instructed all their foreign suppliers to attach a copy of the inspection checklist conducted on the empty container/trailer to the inside of the front door to validate against the arrival condition. Orange shrink-wrap as well as tamper proof tape is used on all U.S. bound shipments.

There are four employees responsible for the sealing of containers: the packing area manager, a security guard, the "lead loader" and the driver. All four sign their names next to the seal number on the manifest. The employees must use a seal verification and inspection process (view, verify, tug and twist) when affixing a seal to a container. There are signs posted at each of the loading doors with pictures and examples of the correct seal verification and inspection process.

The Foreign Manufacturer uses dock locking arms for container storage. The dock locking arm anchors the container chassis against closed dock doors to prevent unauthorized access and the loaded container from being moved during while at the loading facility.

A foreign manufacturer or consolidation facility must receive approval from the Importer's overseas representative before cargo can be loaded into a container. The Importer's representative must be present at the factory to observe the container inspection and the actual loading and sealing operations.

The Importer's trailers are equipped with roof mounted motion sensors. If a trailer's doors are opened and cargo is manipulated in any way, an alarm notification is sent to the Highway Carrier's dispatchers and driver.

The president of a Highway Carrier places playing cards in various key hiding areas within the company's conveyances. When drivers perform the mandatory 17-point inspection, he/she must find all the hidden cards in order to use the vehicle.

The Highway Carrier utilizes a laser beam to protect company trailers when stored in the yard. The laser is positioned 6 inches from the back of parked trailers. If the beam is broken an intrusion alarm is activated.

The Foreign Manufacturer requires their contracted highway carriers to travel to the U.S./Mexican border in a convoy of four or five trailers at a time. The Foreign Manufacturer has also contracted a security service to follow the convoy to the border in an unmarked vehicle. The two guards in the unmarked vehicle record stops, delays and maintain communication with the Foreign Manufacturer's dispatch team in Mexico. The unmarked vehicle is equipped with a digital video recorder, hard drive, and microphone to record the entire 18 ½ hour trip to the U.S. border. When the convoy reaches the border and clears U.S. Customs and Immigration, the unmarked vehicle returns to the manufacturer's location and the guards prepare a trip report. All reports, including pictures and audio/video recordings are maintained on file by the Foreign Manufacturer for review.

The Company has documented a seal destruction policy in its conveyance security handbook. This policy requires that all used seals be sent to a certified hazardous disposal and destruction facility. Once the seals have been destroyed, the hazardous disposal and destruction facility provides a report of the number of seals destroyed and the process of how they were destroyed. A physical seal inventory audit is also conducted on a weekly basis to ensure that all seal logs are reconciled.

Physical Access Controls

The Importer's domestic manufacturing facility has multiple security stations within the building. At these locations security guards are required to challenge and ask for identification from visitors.

All employees, regardless of position within the company, are required to pass through a metal detector upon entering and departing the container packing area to prevent internal conspiracies.

On-site security guards collect all Company ID cards at the end of each shift. Employees are prohibited from taking their ID cards off company property. This procedure mitigates the possibility that a card will be lost and compromise facility security. This system forces the guards to match each employee with the picture on the ID card. The ID cards are kept in a secure location inside the security booth until the next workday.

An Importer's foreign manufacturer has installed an electronic swipe card/lock box system for access control where sensitive trade documents are stored. Only selected managers are given access cards to this secure room. The manager must pass through a manned security desk and swipe the access card to open the lock box which holds the manual key.

If at any point an employee needs to enter a room requiring a physical key, the employee must swipe his Company ID to gain access to a secure lock box containing the designated key to the room.

All visitors' driver licenses are electronically scanned at the Importer's facility and a computer program is used to determine authenticity.

A temporary and numbered visitors badge is issued and a sign-in sheet is maintained by the Importer's reception personnel. All visitors are given a safety and security pamphlet which lists general company safety and security rules that need to be followed while on the premises.

Personnel at the Company's reception area are provided with a hidden duress (panic) button that can be used to alert Company and community law enforcement personnel to a security threat.

The Importer utilizes a third-party software system to manage, design, and plan their physical key inventory. This system ensures that each in-house-produced key is unique. The system tracks all keys in circulation and assigns each authorized employee a key.

The Foreign Manufacturer creates new visitor badges once it is determined that twenty-five percent of the current visitor badges have been lost or damaged.

Physical Security

The Importer's domestic facility has been equipped with a feature that allows the security force to shut down vehicle exits from the facility by electronically closing gates and activating tire puncturing devices.

The Importer uses unmarked security vehicles to patrol the numerous employee and visitor parking areas.

The Importer's facility is inspected three times a day by company security force personnel. The Importer uses an electronic Security Information Reporting System (SIRS) to notify the chief of security and other senior management personnel of any security breaches as soon as they are discovered.

The Importer's foreign business partner's manufacturing facility is located on a large lake that forms part of the border between Germany and Switzerland. In addition to a physical fence, the facility perimeter is also equipped with an invisible electronic fence line that alerts the security force of a possible intruder. The perimeter fencing is also equipped with sensors that detect if the fence has been cut.

A Foreign Manufacturer has installed laser sensors in remote areas of the facility. These sensors help secure those areas of the perimeter of the facility that are inaccessible to security patrols.

An Importer has developed a monitoring platform that incorporates optical light beams that automatically detect the presence of an intruder who might attempt to gain access to the manufacturing facility alongside a train. Once activated, the system sets off an audible alarm at the gate and inside the security command center. The guards also have the ability to speak to the person through a loudspeaker system.

The inbound receiving areas at the Importer's manufacturing plant are kept secured by a double locking door system. The exterior door is locked once the truck and trailer enters the holding area and the interior door is then opened to permit commercial vehicles to park at a loading bay.

The entire Foreign Manufacturer's facility is enclosed by perimeter fencing equipped with infrared sensors to prevent unauthorized access.

The Foreign Manufacturer's external shipping door is assembled in such a way that opening the door requires a security guard outside and a shipping clerk inside the facility to open it.

All of a Foreign Manufacturer's security guard's radios are equipped with a body alarm function, which can be activated by guards during an extreme emergency. When this button is depressed an alert is sent to all guards on duty and the command center. The command center has a direct hotline to the local police department.

The Importer's security force has a K-9 unit onsite. The K-9 unit consists of six trained guard dogs with handlers. The guard dogs and their handlers patrol the perimeter of the facility during working hours.

The Importer's headquarters reception area has multiple glass meeting rooms that can be viewed by the security staff. The enclosed glass rooms allow the Importer's employees to conduct business such as applicant interviews with visitors without providing further access to the facility.

The Foreign Manufacturer's cargo handling area is equipped with multiple interior infrared security alarm beams to detect unauthorized access. In addition to the general alarm contacts, the photo eye beam alarm system is activated in the warehouse after business hours and monitored by a contract security company.

The Foreign Manufacturer's property fence line is duplicated resulting in a dual fence that forms a wide security barrier. The bottom of the fence is buried one foot under ground to deter underground access to the facility.

The foreign manufacturer has installed security guard view towers at each corner of the facility's perimeter. The towers are manned at all times and allow the security staff to monitor activities inside and outside the property.

Personnel Security

The Importer requires that all business partners provide a monthly master list of employees and provide immediate notification when their employees are hired or terminated. This procedure ensures the only authorized business partner's employees are authorized to enter the Importer's manufacturing facilities.

Security Training/Threat Awareness/Outreach

The Importer conducts an annual security awareness seminar (modeled on the C-TPAT Security Seminar) for its U.S-.based suppliers, customers, and other business partners. In 2008, 250 separate entities were invited to this training.

The Importer's website homepage contains a direct link to the C-TPAT security website.

There are four levels of C-TPAT training offered by the Company: management and supervisors; shipping and receiving personnel; internal personnel dealing with contractors; and hourly staff. All employees receive formal and documented training on security/threat awareness. This training includes ways to improve the physical security of the facility, challenging unidentified persons on the premises, and maintaining a safe work environment.

The Importer has an on-line training portal. This training portal requires unique user names and passwords. Employees are trained on the purpose of C-TPAT and C-TPAT security guidelines and criteria. All newly hired employees are given a 90-minute formal presentation on the C-TPAT program and a log is maintained for all training sessions. Managers of specific departments are sent an e-mail in the event employees have not completed mandatory training via the training web site. After a training session is completed, employees receive a written Certificate of Completion from the Company.

Security employees in the Importer's shipping and receiving areas receive additional training that must meet the standard for the local foreign government's Department of Industry and Trade. This training includes instruction in conveyance security and incident reporting procedures, in addition to emergency response practice drills.

An Importer has a continuity of operations plan in place to ensure 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.

A suggestion box has been installed in the facility so that employees can make security suggestions and report anomalies to management. Monthly security reminders are sent out to all personnel via the company's email system.

The Importer has instituted a program to place C-TPAT placemats on all food service trays in the employees' cafeteria. These placemats provide employees with up-to-date information on the C-TPAT program and the company's role in supply chain security.

The Importer's overseas manufacturing facility security staff is licensed by the foreign government. Security guards receive forty hours of general security training and an additional thirty-two hours of site-specific training that is given by the U.S. Importer's management representatives. Guards also receive three full days of C-TPAT training and orientation.

A Foreign Manufacturer's facility displays container security inspection posters outlining the C-TPAT recommended container inspection process throughout its facility.

The Importer maintains a proprietary internal television network. This network is used to relay pertinent information to employees at the Company's U.S. facilities. The network is routinely used by management to deliver information on the C-TPAT program and supply chain security. This system is also used to reinforce classroom security training and keep employees current and up to date on Company security policies and procedures.

The Importer issues security advisories to its worldwide business partners. Security issues are also sent on a daily basis to employees via e-mail, notice boards and in first line supervisor briefings.

A yearly security awareness assessment, given annually to a random sample of employees, is used by an Importer's management staff to gauge employees' general security awareness and identify any security issues that need greater attention.

An Importer regularly conducts table-top exercises to address possible security breaches in the Company's supply chain. The Importer has implemented a "Quick Response Team" that can be deployed immediately after suspicious activity is discovered involving the movement of their product.

An Importer has established a situation matrix chart to address possible incidents (i.e., incorrect seals, container tampering or unexpected cartons) in arriving cargo. The oversize easy-to-read chart is posted on the wall of each warehouse facility. The table provides possible discrepancies, and persons to notify.

The Importer has a security assessment team whose function is to conduct periodic "penetration assessments" of the Company's supply chain security procedures. Company representatives make unannounced visits to an overseas facility and see if they can gain entry.

A C-TPAT based Best Practices Catalog has been developed by the Importer. A yearly site assessment of the company's U.S. manufacturing facility is conducted to ensure that security procedures and guidelines remain consistent with the C-TPAT program security requirements and/or recommendations.

The Importer utilizes a variety of measures to ensure that its employees are notified of the current Department of Homeland Security threat level. The Company uses digital message boards at all building entrances, CCTV monitors, e-mail notifications, the Company web site, and a toll-free phone number to notify employees of any changes in the threat level.

The Importer has instituted a "Speak Up" program, a direct communication channel to the president of the company to address security issues via a confidential written form.

An Importer has two forums that allow concerned employees the opportunity to express security concerns. Company personnel can call a toll free hotline that is administered by a neutral third-party or send messages via an internet based forum. Both forums provide the same opportunity to express safety concerns, and present security issues.

All of an Importer's U.S. facilities conduct security drills and exercises that are designed to test the effectiveness of the company's workforce to react to a security related incident. The security drills and exercises include the involvement of vendors, contractors and local, state and federal agencies, including CBP and the US Coast Guard (USCG). The drills are conducted on a quarterly basis and focus on the initiation and reporting of a security related incident. An annual company-wide security exercise, which is broader in scope than each facility's individual exercises, is also conducted.

Web-based security awareness training is available to all of a Foreign Manufacturer's employees' 24-hours, seven-days a week and it is offered in three languages. The training modules provide instruction on container and seal inspections, parcel and mail screening, as well as a basic overview of the C-TPAT program. The Company also displays C-TPAT awareness posters throughout the facility which are printed in several languages. Once employees have completed the C-TPAT awareness training, they are issued a button which displays the C-TPAT logo and it is worn as part of their uniform. Management offers a monetary award for exhibiting good work practices including recommendations and informing management of any security issue. Employees are penalized for not following company security guidelines. Severe violations result in disciplinary action up to and including termination.

All security incidents are documented and recorded on a central database by the Importer. The database is analyzed by the Company's security department for patterns and to determine if changes to existing security policies and/or procedures are warranted.

The Importer has designated one month a year as "Security Month" to further promote security awareness among its employees. Numerous security workshops are conducted during this month and outside law enforcement authorities are invited to provide additional security information/training.

The Importer has established a global communication system to contact all employees and contractors remotely via tele-conferencing technology on a quarterly basis to discuss security issues and provide information on recent security threats. The process allows the security team to offer advice as to how the issues can be prevented in the future and allows all parties to share ideas and offer input as a team.

Procedural Security

A Foreign Manufacturer utilizes a bio-thermal intrusion alarm system to protect access to sensitive business documents.

The Importer utilizes a global SAP network to generate all written orders for import and export. A specific Company policy regulates this process and requires all orders to be generated within the SAP environment. This system permits only authorized stakeholders to view relevant shipping information. Every order entered into this system is vetted against the Denied Persons list and the U.S. Office of Foreign Assets Control (OFAC) lists.

An Importer's foreign facility receives in excess of 15,000 mail parcels per day. The company operates its own post office which is located just outside the premises.

A Global Trade System (GTS) automatically screens purchase orders for restricted parties and internationally sanctioned destination countries. The system blocks such orders until reviewed by an export sales expert for final decision.

If a particular shipper delivers an unauthorized quantity or product, the system will automatically log this information in the Importer's SAP program. Management personnel review this data, along with comments from various departments on a quarterly basis. Senior management uses this information when considering contract renewal with specific suppliers and/or vendors.

The weekly use of an Importer's Quality Audit Form insures consistent and thorough management oversight of daily operations by providing a documented means in which shipment problems can be identified and resolved.

The Importer has implemented lock boxes for all sensitive documentation that has to be shredded to safeguard business information.

The Foreign Manufacturer utilizes an automated loading module called the Automatic Truck Loading System (ATLS). A robotized lift-truck is mounted on a transfer platform that travels sideways, allowing it to move from various dock doors and enter trailers to deposit the loads. Once the platform has aligned with the appropriate door, the ATLS automatically measures the length and dimensions of each trailer with a laser distance meter to optimize the load pattern. If the dimension of the container being loaded is inaccurate the ATLS immediately rejects the container and stops the loading process to electronically notify management of the issue.

The Importer uses the container seal number as the shipment tracking (invoice/bill of lading) number. This helps to ensure the seal number is always stated on the shipping documents and helps each partner in the supply chain to verify that the original seal is intact.

Seal usage (seal number/trailer number/driver/date) and seal removal information (name of removing official/badge id/date/location/second seal number) are also notated on a run sheet in a special section entitled “Seal Usage Index Card”. A run sheet is a document supplied to all drivers for each pickup/delivery, and used by the company to capture information relevant to the driver’s trip such as destination, trailer number, route used, border crossed, odometer reading, and expenses incurred. Also included on the run sheet is a C-TPAT high security inspection that consists of 17 examination points drivers are required to perform as part of their pre-trip inspection

Information Technology (IT) Security

The Foreign Exporter's automated systems server room is secured by a biometric fingerprint door lock. Only IT managers are allowed access into the room.

An Importer has identified a threat to its IT system data backups due to high earthquake activity and has placed the remote data backup center in a location that has a low incidence of earthquakes. The server room is in an earthquake proof building protected by a halon gas equipped fire extinguishing system.

IT managers perform quarterly access rights reviews for employees. In addition, they review access rights on a monthly basis for contractors to safeguard the manufacturing facility's electronic business data.

An agreement of liability for the use of an Importer's information systems is renewed each time a user changes a password.

A retina scan is required to access the Foreign Manufacturer's computer system. There is a secure door for access to the mainframe computer. The door will only allow one person to enter. No one can follow or "piggy back" the person entering the door, or the secondary door to the mainframe computer will not open.

The Importer's employee desktop computers do not contain hard drives capable of copying company data onto a CD or disk. Employees must gain supervisory approval to copy data. The Importer has a dedicated IT office which can copy company business data once supervisory approval is obtained. This process allows the Importer to limit access to new research and development information and assist in identifying abuse of improper access, tampering or alteration of their business data.

Within the Foreign Manufacturer's production facility, each office workstation contains a photo of the employee who is assigned to that work area, allowing management to be aware of any unauthorized computer terminal usage.

The Importer uses electronic password protected purchase orders with its foreign supplier. Only five company officers in the foreign supplier's headquarters have access to the password.

The Importer does not permit employee use of "blackberry" type PDA's due to the possibility of Company emails or business data being read while on the service providers computer system. The IT server room is unmarked to provide additional security to the company's business data.

An Importer's employees are trained and tested in computer and facility security by being required to take a daily "e-test" on their computers. Employees must pass the "e-test" before being able to log on to the computer terminal.

Upon logging into an Importer's computer system, a security warning message is displayed and the user must accept to continue. Disciplinary action is taken against any employee violating the policy.