CTPAT SECURITY AUDIT OVERVIEW

CONTAINER & TRAILER SECURITY

Container and trailer integrity must be maintained to protect against unauthorized products/persons. At the point of loading, vendors must have procedures in place to properly seal and maintain the integrity of the shipping containers/trailers. Procedures must be in place to verify the physical integrity prior to loading including reliability and the locking of door mechanisms. An inspection process is required for containers and for trailers.

CONTAINER INSPECTION	TRAILER INSPECTION	CONTAINER & TRAILER STORAGE	CONTAINER & TRAILER SEALS
Front Wall Left Side Right Side Floor Ceiling Inside/Outside Doors Outside/Undercarriage	Fifth Wheel Area Exterior Front/Sides Rear Bumper/Doors Front Wall Left Side and Right Side Floor Ceiling/Roof Inside/Outside Doors Outside/Undercarriage	Containers must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for preventing and reporting unauthorized entry in containers/trailers or container/trailer storage areas.	A high security seal must be affixed to all loaded inbound US containers and trailers. All seals must meet or exceed the current PAS ISO 17712 standard for high security seals. Written procedures must stipulate how seals are to be controlled and affixed, including recognizing and reporting compromised seals or containers/trailers.

PHYSICAL SECURITY

FENCING/GATES/GATE HOUSES	PARKING	BUILDING STRUCTURE	LOCKING DEVICES & KEY CONTROLS	LIGHTING	ALARMS SYSTEMS & VIDEO SURVEILLANCE CAMERAS
Packed product stored outside the exterior yard area should be enclosed with fencing and/or should be secured otherwise to prevent unlawful access.	Defined parking area for private vehicles which are separate from the shipping, load dock and cargo areas.	Major access and security points shall be lit (lights in all critical areas must be functioning).	Security systems shall cover all critical areas (all external doors, loading docks, productions areas, etc.).	Major access and security points shall be lit (lights in all critical areas must be functioning).	The facility is protected by security systems and/or security personnel. Security systems are tested periodically and monitored.

PHYSICAL ACCESS CONTROLS

Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.

EMPLOYEES/ VISITORS	DELIVERIES	CHALLENGING & REMOVING UNAUTHORIZED PERSONS	PRE-EMPLOYMENT VERIFICATION	BACKGROUND CHECKS/INVESTIGATIONS - EMPLOYEES	PERSONNEL TERMINATION PROCEDURES
Employees-Identification in place for positive identification and access control purposes. **Visitors**- must present photo identification upon arrival. All visitors should be escorted.	Proper ID and/or photo identification must be presented upon arrival. Arriving packages and mail should be screened before being distributed.	Identify, challenge and address unauthorized/ unidentified persons.	Employment history and references must be verified prior to employment	Background checks and investigations should be conducted on new employees. Periodic checks and reinvestigations should be performed on current employees.	Companies must have procedures in place to remove identification, facility access and systems access for terminated employees.

PROCEDURAL SECURITY

Documented processes to verify that information used in the clearing of merchandise/cargo, legibility, completeness and accuracy, that documents are protected against inaccuracies, and that computer access and information is safeguarded. Manifesting procedures shall be in place to verify information received from business partners is reported accurately and timely. Shipping and receiving procedures shall be in place to verify departing cargo is reconciled against cargo manifest, that all information is accurate. Drivers delivering or receiving cargo should be identified before cargo is received or released. Cargo must be tracked and traced.

CARGO DISCREPANCIES	INFORMATION TECHNOLOGY SECURITY	SECURITY TRAINING & THREAT AWARENESS
Must be resolved and/or investigated appropriately so all shortages, overages and any discrepancies are reported to Customs and/or appropriate law enforcement agency.	Written computer security policies/procedures are established. Individual accounts and passwords are created for users to access the system. Passwords are changed periodically (at least every 90 days). Access to computer systems is monitored and reviewed periodically.	Security awareness programs should be in place in the following areas: threat awareness, security procedures, cargo integrity, internal conspiracies, protecting access controls, container security and facility security.

SUPPLY CHAIN SECURITY BEST PRACTICES

To assist our supply chain partners to meet or exceed the CTPAT guidelines, please note the following examples of supply chain security best practices exercised by CTPAT member companies.

SECURING EMPTY CONTAINERS	Driver conducts and documents inspection of container using a checklist prior to leaving and signs after the seal is affixed by security, verified and documented by both parties.
SECURING FULL CONTAINERS	Digital picture taken of the back of the loaded container before doors are closed and sealed. Pictures transmitted to port terminal operator and import in the United States.
INSPECTING & WEIGHING CONTAINERS	Weigh containers/ trailers before and after loading. Shipping Manager, Guard or Driver should be present for loading and sign off after verifying inspections are completed. If container is not immediately loaded padlocks and plastic seals are placed on the doors until the container is loaded.
CONTAINER/TRAILER STORAGE	Inventory management system is used to track and monitor empty containers staged in factory yard.
PHYSICAL SECURITY	Manufacturer maintains an alarm system with laser sensors in remote areas of the facility. Shipping doors are assembled in a way which requires a security guard outside and a shipping clerk inside to open it.
VISITORS	Issue a numbered badge at reception after identity and appointment is verified. Company establishes a visitor's database tracking visitor address and identity information. Visitors go through metal detector and bags x-rayed and searched.
ACCESS CONTROLS	All employees are required to pass through a metal detector when entering and exiting the facility. Employees must use company ID card to gain access to a secure lockbox containing keys to secure rooms. Reception areas to have hidden panic button for security threats.

SPORTSMAN'S GUIDE