

CTPAT – SECURITY REQUIREMENTS SUMMARY

Following is a general summary of the C-TPAT security requirements.

(a) Container Security

Containers that are loaded and bound for the United States must undergo certain procedures to protect against the introduction of unauthorized materials and or persons. Foreign factories' shipping supervisors or managers must supervise the loading of containers destined to Tractor Supply Company facilities. The foreign factories must implement a container security process. This process is to include a 7-point Container Security Check, validating the quantity of cargo being shipped against the Purchase Orders received from Tractor Supply Company, securing the container with a high security seal (PAS ISO 17712 compliant through U.S. Customs), and finally all containers are to be stored in a secure area to prevent any unauthorized manipulation or access.

In the event the foreign facility discovers security issues, compromised seals or containers that may affect the security of the Tractor Supply Company supply chain, they must alert the Tractor Supply Company Strategic Sourcing Department, local law enforcement and/or local Customs.

(b) Container Seals

At the point of stuffing, procedures must be in place to properly seal and maintain the security of the container. After stuffing the containers, a high security seal (PAS ISO 17712) must be affixed to the container. Procedures must be in place that keep the seals in a secure area such as a locked safe, or file cabinet and assign a designated employee to control and distribute the seals. In the event that a container seal is compromised, procedures must be in place to alert management, local law enforcement and/or local Customs.

(c) Container Inspection

To ensure the integrity of the container, procedures should be in place to verify the physical integrity of the container. Prior to stuffing the container, a 7-point security inspection should be conducted on all containers that are destined to the United States. This 7-point inspection should include:

- Front wall;
- Left side;
- Right side;
- Floor;
- Ceiling/Roof;
- Inside/outside doors;
- Outside/Undercarriage.

In examining these areas, look for the following discrepancies.

- Holes;
- Cuts;
- Two-toned areas on the container/trailer;
- Unusual welding to an area of a container/trailer. Welding should be visible on the inside as well as the outside of the container;

- Blockage of the undercarriage of the container/trailer (beams should be exposed. No smooth surfaces should exist under the container);
- Different color bonding material on locking mechanisms. This is a good indication that locks have been refashioned;
- Blocks and vents being obstructed. The blocks and vents should always be visible;
- Floors should be flat. There should never be different floor heights.

(d) Container Storage

Containers must be stored in a secure area to prevent unauthorized access and/or manipulation. Vendors must implement procedures for reporting and neutralizing unauthorized entry into containers or container storage areas.

(e) Physical Access Controls

Vendors must implement access controls to 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.

(f) Employees

An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to those secure areas needed for the performance of their duties. Vendor's management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented.

(g) Visitors

Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and visibly display temporary identification.

(h) Deliveries

Proper identification and/or photo identification must be presented for documentation purposes upon arrival by all.

(i) Challenging and Removing Unauthorized Persons

Procedures must be in place to identify, challenge and address unauthorized persons in the facility.

(j) Personnel Security

Vendors shall implement processes to screen prospective employees and to periodically check current employees. Application information, such as employment history and references must be verified prior to employment. Vendors shall conduct background checks and investigations on prospective employees in accordance with all applicable laws, foreign and domestic. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

(k) Personnel Termination Procedures

Vendors must have procedures in place to remove identification, facility, and system access for terminated employees.

(l) Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.

(m) Documentation Processing

Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. Documentation control must include safeguarding computer access and information.

(n) Manifesting Procedures

To help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and timely. This sounds like instructions to TSC not its foreign vendors.

(o) Shipping & Receiving

Vendor must reconcile cargo against information on the cargo manifest prior to shipping. The cargo must be accurately described, and the weights, labels, marks and piece count indicated and verified. Departing cargo must be verified against Purchase Orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released.

(p) Cargo Discrepancies

All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. Customs and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected - as appropriate.

(q) Security Training and Threat Awareness

Vendors must have procedures in place to remove identification, facility, and system access for terminated employees. A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists at each point in the supply chain. Employees must be made aware of the procedures the company has in place to address a situation and how to report it. Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail.

Additionally, specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation.

Physical Security

Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Importers should incorporate the following C-TPAT physical security criteria throughout their supply chains as applicable.

(r) Fencing

Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All fencing must be regularly inspected for integrity and damage.

(s) Gates and Gate Houses

Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

(t) Parking

Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas.

(u) Building Structure

Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

(v) Locking Devices and Key Controls

All external and internal windows, gates and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.

(w) Lighting

Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.

(x) Alarm Systems & Video Surveillance Cameras

Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

(y) Information Technology Security

Password Protection: Automated systems must use individually assigned accounts that require a periodic change of password. IT security policies, procedures and standards must be in place and provided to employees in the form of training.

(z) Accountability

A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.