C-TPAT Requirements, Exporters to U.S.

Business Partner and Non-U.S. Snap-on Facilities Requirements

Importers must ensure business partners develop security processes and procedures consistent with the C-TPAT security criteria to enhance the integrity of the shipment at **point of origin**. Periodic reviews of business partners' processes and facilities should be conducted based on risk, and should maintain the security standards required by the importer. For those business partners eligible for C-TPAT certification (carriers, ports, terminals, brokers, consolidators, etc.) the importer must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these business partners are or are not C-TPAT certified.

For those business partners not eligible for C-TPAT certification, importers must require their business partners to demonstrate that they are meeting C-TPAT security criteria via written/electronic confirmation (e.g., contractual obligations; via a letter from a senior business partner officer attesting to compliance; a written statement from the business partner demonstrating their compliance with C-TPAT security criteria or an equivalent WCO accredited security program administered by a foreign customs authority; or, by providing a completed importer security questionnaire).Based upon a documented risk assessment process, non-C-TPAT eligible business partners must be subject to verification of compliance with C-TPAT security criteria by the importer.

Security Procedure, Point of Origin

Importers must ensure business partners develop security processes and procedures consistent with the C-TPAT security criteria to enhance the integrity of the shipment at point of origin. Periodic reviews of business partners' processes and facilities should be conducted based on risk, and should maintain the security standards required by the importer.

Security Procedure, Participation / Certification in Foreign Customs Administrations Supply Chain Security Programs

Current or prospective business partners who have obtained a certification in a supply chain security program being administered by foreign Customs Administration should be required to indicate their status of participation to the importer.

Container Security, General

Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At point of stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers. A high security seal must be affixed to all loaded containers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

Container Security, Container Inspection

Procedures must be in place to verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers: Front wall, Left side, Right side, Floor, Ceiling/Roof, Inside/outside doors, Outside/Undercarriage

Container Security, Container Seals

Written procedures must stipulate how seals are to be controlled and affixed to loaded containers - to include procedures for recognizing and reporting compromised seals and/or containers to US Customs and Border Protection or the appropriate foreign authority. Only designated employees should distribute container seals for integrity purposes.

Container Security, Container Storage

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

Physical Access Controls, 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. Company 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.

Physical Access Controls, Visitor Controls

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

Physical Access Controls, Deliveries (including mail)

Proper vendor ID and/or photo identification must be presented for documentation purposes upon arrival by all vendors. Arriving packages and mail should be periodically screened before being disseminated.

Physical Access Controls, Challenging and Removing Unauthorized Persons

Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

Personnel Security, Pre-Employment Verification

Application information, such as employment history and references must be verified prior to employment.

Personnel Security, Background checks / investigations

Consistent with foreign, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

Personnel Security, Personnel Termination Procedures

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

Procedural Security, 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.

Procedural Security, Shipping & Receiving

Arriving cargo should be reconciled against information on the cargo manifest. The cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified. Departing cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released.

Security Training and Threat Awareness

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, 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.

Physical Security, 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.

Physical Security, Parking

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

Physical Security, Building Structure

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

Physical Security, 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.

Physical Security, 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.

Physical Security, Alarms 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.

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.

Information Technology Security – 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.