DRAFT 2
Created on 12/3/2004 10:33 AM

C-TPAT Security Standards

Importers

Importers must conduct a comprehensive assessment of their international supply chains based upon the following C-TPAT security standards. Appropriate security measures must be implemented and maintained throughout the importer's supply chains - based on risk.[1] Where an importer outsources or contracts elements of their supply chain, such as a foreign facility, conveyance, domestic warehouse, or other elements, the importer must work with these business partners to ensure that pertinent security measures are in place and adhered to by their direct/contracted business partners. The supply chain for C-TPAT purposes is defined from point of origin (manufacturer/supplier/vendor) through to point of distribution.

C-TPAT recognizes the complexity of international supply chains and endorses the application and implementation of security measures based upon risk analysis. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model.

Business Partner Requirement

Importers must have written and verifiable processes for the selection of business partners including manufacturers, product suppliers and vendors. Processes must include the verification of a written security questionnaire or security report submitted by the business partner. For those business partners eligible for C-TPAT certification (carriers, terminal operators, brokers and consolidators, etc.) the importer must have documentation indicating that these business partners are/are not C-TPAT certified.

- **Security procedures**
  Importers must require current and prospective business partners, not already C-TPAT certified, to submit a written response to a security questionnaire regarding their current security procedures. Questionnaires and responses must be reviewed, and if weaknesses are noted, the importer should implement an appropriate plan of action, based on risk, that will assist the business partner in improving their security. Questionnaires and responses received must be filed and produced upon request by CBP. It is imperative that business partners outline their current security practices and procedures for their C-TPAT importer so potential supply chain weaknesses can be identified and appropriately corrected. Through these questionnaires, importers can more easily identify if outsourcing occurs at any point in their supply chain and if C-TPAT security standards are being met or exceeded by the entity handling their merchandise.

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

- **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.

[1] Importers shall have a documented and verifiable process for determining risk throughout their supply chains based on their business model (i.e., volume, country of origin, routing, potential terrorist threat via open source information, etc.)

- **Other internal requirements for selection**
  Internal requirements, such as financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed, should be addressed by the importer. Internal requirements should be accessed against a risk-based process as determined by an internal management team.

Container Security

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

- **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 Seals**
  Written procedures must stipulate how seals are to be secured, logged, and affixed to loaded containers and verified throughout the supply chain - to include procedures for recognizing and reporting compromised seals or seal discrepancies to US Customs and Border Protection or the appropriate foreign authority. Only designated employees should handle and distribute container seals for integrity purposes.

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

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**
  An employee identification system must be in place for positive identification and access control. Employees should only be given access to areas needed for the performance of their duties.

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

- **Deliveries (including mail)**
  Vendors must present photo identification for documentation purposes upon arrival. Arriving packages and mail should be screened before being disseminated.

- **Challenging and Removing Unauthorized Persons**
  Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

- **Securing Physical Access**
  Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges. The issuance, removal and changing of access devices (e.g. keys, key cards, etc.) as necessary.

Personnel Security

Processes must be in place to screen prospective employees and to periodically check current employees.

- **Pre-Employment Verification**
  Application information, such as employment history and references must be verified prior to employment.

- **Background checks / investigations**
  Consistent with foreign, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic background checks and reinvestigations should be performed.

- **Personnel Termination Procedures**
  Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

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.

- **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.

- **Manifesting Procedures**
  Procedures must be in place to ensure that information received from foreign suppliers is reported accurately and timely.

- **Shipping & Receiving**
  Arriving cargo should be reconciled against advance 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.

- **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 activities are detected.

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 the response to 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 standards throughout their supply chains as applicable.

- **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.

- **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.

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

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

- **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.

- **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.

- **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.

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