welcome to

Telect's Minimum Security Criteria for Customs-Trade Partnership Against Terrorism (C-TPAT) Foreign Manufacturers Training Presentation

Telect

Minimum Security Criteria Scope

- Designed to be the building blocks to institute effective security practices designed to optimize supply chain performance to mitigate the risk of loss, theft, and contraband smuggling that could potentially introduce terrorists and implements of terrorism into the global supply chain.
- The determination and scope of criminal elements targeting world commerce through internal conspiracies requires companies, and in particular, foreign manufacturers to elevate their security practices.
- For the purposes of C-TPAT, supply chain is defined from the point or origin (including packaging and stuffing) to the point of final destination.

Telect

Requirements of Foreign Manufacturer

- Conduct a full assessment once a year at a minimum, or as circumstances dictate during periods of heightened alert, security breach or incident.
- The assessment is a complete analysis of your international supply chain (which includes your business partners for outsourcing, contract manufacturing, installation, storage and transportation providers) to ensure that pertinent security measures are in place.

Requirements of Foreign Manufacturers

- Appropriate security measures must be implemented and maintained throughout the Foreign manufacturer's supply chains.
- Manufacturer/Supplier's must have a viable and documented process to determine risk in all supply chains based on the 8 elements listed below.
  - Business Partner Requirements
  - Container and Trailer Security
  - Physical Access Controls
  - Personnel Security
  - Procedural Security
  - Physical Security
  - Information Technology Security
  - Security Training and Threat Awareness

Business Partner Requirements

- Have a written and verifiable process for the selection of business partners including, carriers, other manufacturers, product suppliers and vendors (parts & raw material suppliers, etc.)
- Security Procedures for those business partners eligible for C-TPAT certification (carriers, importers, ports, terminals, brokers, consolidators, etc.) and must obtain documentation (such as the C-TPAT SVI Number (Status Verification Interface)) indicating whether these business partners are or are not C-TPAT certified. If not then documentation proving they meeting an equivalent World Customs Organization accredited security program administered by a foreign customs authority
- If neither a SVI or other certified security program is available then certification the partner is demonstrating that they are meeting the C-TPAT security criteria via written/electronic confirmation (e.g. contractual obligation; a written statement from the business partner demonstrating their compliance with C-TPAT security criteria
- A risk assessment process, non C-TPAT eligible business partners must be subject to verification of compliance with C-TPAT security criteria by the foreign manufacturer
- You must ensure that 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, assembly or manufacturing and review the business partner based on risk and that are maintaining the security standards required by you.
- US bound shipments should be monitored that C-TPAT carriers are being used, or non-C-TPAT carriers that they are meeting the C-TPAT security criteria as outlined above for business partner requirements.

Telect

Container and Trailer Security

- Container and trailer integrity, if applicable, must be maintained to protect against the introduction of unauthorized material and/or persons
- At the point of stuffing procedures must be in place to properly seal and maintain the integrity of the shipping containers and trailers
- Shipments bound for the U.S. must be affixed with a PAS ISO 17712 (details can be found on the Internet)
- Containers must be inspected for physical integrity prior to loading based on the following seven-point inspection process:
  - Front Wall
  - Left Side
  - Right Side
  - Floor
  - Ceiling/Roof
  - Inside/Outside Doors
  - Outside/Undercarriage

Container and Trailer Security Continued

- Procedures must be in place to verify the physical integrity of the trailer structure prior to stuffing which must include the reliability of the locking mechanisms of the doors. The following ten-point inspection process is recommended:
  - Fifth wheel area – check natural compartment/skid plate
  - Exterior – front/sides
  - Rear – bumper/doors
  - Front Wall
  - Left Side
  - Right Side
  - Floor
  - Ceiling/Roof
  - Inside/outside doors
  - Outside/Undercarriage
- Seals integrity is a crucial element of a secure supply chain and is a critical part of a foreign manufacturers' commitment to C-TPAT. High security seals must be affixed to all full loaded containers and trailers. Written procedures must stipulate how seals are controlled and affixed to conveyance and must include recognizing and reporting compromised seals and/or containers/trailers to the appropriate foreign authorities. Only designated employees should distribute seals.
- Containers and trailers must be stored in a secure area to prevent unauthorized access and/or manipulation.

Physical Access Controls

- Access controls prevent unauthorized entry to facilities, maintain control of employees & visitors, and protect company assets
- Employees
  - An identification system must be in place to positively identify an employee
  - Should only be given access to those secure areas needed to perform their job
  - Management or Security personnel must adequately control the issuance and removal of employees, visitor and vendor identification badges
  - Procedures for the issuance, removal and changing of access devices (keys, key cards, etc.) must be documented
- Visitors
  - Must present photo identification
  - Sign in/out logs must be kept and retained
  - Must be escorted
  - Should visibly display a temporary identification badge which is assigned to them and logged
- Deliveries
  - Proper vendor/carrier ID photo identification must be presented upon arrival by all vendors
  - Arriving packages and mail should be periodically screened before being disseminated
  - Sign in/out log must be kept and retained for all vendors and carriers
- Challenging and Removing Unauthorized Person
  - Procedures must be in place to identify, challenge and address unauthorized/unidentified persons
  - Employees should be empowered to challenge all unknown persons not wearing a visitor badge
  - Employees should be aware of who to contact in case of an unauthorized situation

Personnel Security

- Process must be in place to screen prospective employees and to periodically check current employees
- Application information, such as employment history and references must be verified prior to employment
- Consistent with foreign regulations, background checks and investigations should be conducted for prospective employees.
- Procedures must be in place to remove identification, facility, and system access for terminated employees immediately upon termination.

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
- 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, which includes safeguarding computer access and information
- Procedures to ensure the information received from business partners is reported accurately and timely must be in place
- Departing cargo should be reconciled against cargo manifest accurately depicting part description, marks & piece count, weights, labels and verified against purchase or delivery orders
- Drivers delivering or receiving cargo must be positively identified before cargo is received or released
- All shortages, overages and other significant discrepancies or anomalies must be resolved and/or investigated appropriately
- Customs or other law enforcement agencies must be notified if anomalies, illegal or suspicious activities are detected – as appropriate

Physical Security

- Cargo handling & storage facilities in international locations must have physical barriers & deterrents that guard against unauthorized access
- Perimeter fencing should enclose the areas around cargo handling and storage facilities and regularly inspected for integrity and damage
- Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored and kept to a minimum for proper access and safety
- Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas
- Buildings must be constructed of materials that resist unlawful entry and must be maintained and periodically inspected and repaired as necessary
- All external and internal windows, gates and fences must be secured with locking devices and management or security personnel must control the issuance of all locks and keys
- Adequate lighting must be provided inside and outside the facility including entrances, exits, cargo handling, storage areas, fence lines and parking areas
- 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

- Automated systems must use individually assigned accounts (user ID's) that require a periodic change of password
- 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
- IT security policies, procedures and standards must be in place and provided to employees in the form of training
- Written procedures outlining employee access and deactivation upon terminated must be in place

Security Training and Threat Awareness

- A threat awareness program should be established and maintained
- Employees should be trained annually at minimum on how to recognize, identify, and report a threat to the supply chain
- Employees should be trained on the threat posed by terrorists and contraband/human smugglers 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
- Employees should be trained on how to recognize internal conspiracies
- Employees should understand the benefits of implementing a recognized Supply Chain Security Program and should be offered incentives for active employee participation

Telect®